(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 2 728 792 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
05.06.2019 Bulletin 2019/23

(21) Application number: **12805120.8**

(22) Date of filing: **27.02.2012**

(51) Int Cl.:
H04L 9/32 *(2006.01)* ***H04L 29/06*** *(2006.01)*

(86) International application number:
PCT/JP2012/054843

(87) International publication number:
WO 2013/001851 (03.01.2013 Gazette 2013/01)

(54) **SYSTEM FOR PROVIDING SETS OF CONTENT AND APPLICATIONS AND CONTROL METHOD THEREFOR, TERMINAL AND CONTROL METHOD THEREFOR, AUTHENTICATION DEVICE AND CONTROL METHOD THEREFOR, PROGRAM, AND INFORMATION STORAGE MEDIUM**

SYSTEM ZUR BEREITSTELLUNG VON SÄTZEN VON INHALTEN UND ANWENDUNGEN UND STEUERVERFAHREN DAFÜR, ENDGERÄT UND STEUERVERFAHREN DAFÜR, AUTHENTIFIZIERUNGSVORRICHTUNG UND STEUERVERFAHREN DAFÜR, PROGRAMM UND INFORMATIONSSPEICHERMEDIUM

SYSTÈME DE FOURNITURE D'ENSEMBLES DE CONTENUS ET D'APPLICATIONS ET SON PROCÉDÉ DE COMMANDE, TERMINAL ET SON PROCÉDÉ DE COMMANDE, DISPOSITIF D'AUTHENTIFICATION ET SON PROCÉDÉ DE COMMANDE, PROGRAMME ET SUPPORT DE STOCKAGE D'INFORMATIONS

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **30.06.2011 JP 2011146890**

(43) Date of publication of application:
07.05.2014 Bulletin 2014/19

(73) Proprietor: **Rakuten, Inc.**
Tokyo 158-0094 (JP)

(72) Inventor: **TAKAMI, Shinya**
Tokyo 140-0002 (JP)

(74) Representative: **Hoffmann Eitle**
Patent- und Rechtsanwälte PartmbB
Arabellastraße 30
81925 München (DE)

(56) References cited:
EP-A1- 1 677 205
JP-A- 7 064 912
JP-A- 7 081 521
JP-A- 2001 308 850
JP-A- 2007 036 441
US-A- 5 719 941

EP 2 728 792 B1

Printed by Jouve, 75001 PARIS (FR)

Description

TECHNICAL FIELD

[0001] The present invention relates to a system for providing content or an application (a content or application providing system), a control method for the content or application providing system, a terminal device, a control method for the terminal device, an authentication device, a control method for the authentication device, a program, and an information storage medium.

BACKGROUND ART

[0002] There is known a system for providing a user with content or an application. In such a system, content or an application is downloaded to a terminal device to be used therein. That is, in the terminal device, content, such as an image, a video, an electronic book, or the like, is displayed on a display unit, content, such as music, or the like, is output from a sound output unit, or an application is executed. In other words, a user in a terminal device sees and listens to content, such as an image, a video, music, or the like, reads content, such as an electronic book, or the like, and uses an application.

[0003] With respect to the above described content system, there has been proposed a technique for restricting use of content or an application copied to a terminal device (hereinafter referred to as an "unauthorized terminal device") other than a terminal device (hereinafter referred to as an "authorized terminal device") that is authentically allowed to use the content or application. Specifically, for example, there has been proposed a technique for checking in a server device, a combination of the ID of a terminal device and that of content or an application when using the content or application in the terminal device, with the ID of the terminal device being stored so as to be correlated to the ID of content or an application available for authentic use in the terminal device, so that use of the content or application in a unauthorized terminal device is restricted.

Citation List

Patent Literature

Patent Literature 1: JP 2004-282238 A

[0004] EP-A1-1 677 205 discloses that in a client/server system that authenticates according to a terminal ID, a terminal authentication apparatus is provided that is capable of authenticating a terminal device correctly even if the method of generating a terminal ID has been changed from the old version to a new one, and thus useful as an authentication apparatus for a net TV, mobile phone, on-line network for ATMs, and the like. The apparatus transmits two terminal IDs generated with the generation methods in both old and new versions. The server authenticates from these two terminal IDs according to the ID field of the old and new versions, and additionally updates the ID in the old version to a new one.

SUMMARY OF INVENTION

Technical Problem

[0005] However, according to the above-described technique, in a case where content or an application is copied to an unauthorized terminal device, and the ID of an authorized terminal device is impersonated as the ID of the unauthorized terminal device, it is not possible to restrict use of the content or application in the unauthorized terminal device. As a result, a case may be resulted in which the content or application can be used in a plurality of terminal devices including a single authorized terminal device and one or more unauthorized terminal devices. That is, a case may be resulted in which content or an application can be used in two or more terminal devices, though there is only one authorized terminal device.

[0006] The present invention has been conceived in view of the above, and an object thereof is to provide a content or application providing system, a control method therefor, a terminal device, a control method therefor, an authentication device, a control method therefor, a program, and an information storage medium capable of restricting a terminal device allowed to use content or an application to a single terminal device among one authorized terminal device and one or more unauthorized terminal devices.

Solution to Problem

[0007] The present invention provides a terminal device for a user to use content or an application, connectable for communication to an authentication system according to Claim 1.

[0008] The present invention also provides an authentication device connectable for communication to a terminal device for a user to use content or an application according to Claim 2.

[0009] The present invention also provides a system for providing content or an application including a terminal device for a user to use the content or the application and an authentication system according to Claim 3.

[0010] The present invention also provides a control method for a terminal device for a user to use content or an application, connected for communication to an authentication system according to Claim 13.

[0011] The present invention also provides a control method for an authentication device connected for communication to a terminal device for a user to use content or an application according to Claim 14.

[0012] The present invention also provides a control method for a system for providing content or an application including a terminal device for a user to use the con-

tent or the application and an authentication system according to Claim 15.

[0013] The present invention also provides a program for causing a computer to function as a terminal device for a user to use content or an application, connected for communication to an authentication system according to Claim 16.

[0014] The present invention also provides a program for causing a computer to function as an authentication device connected for communication to a terminal device for a user to use content or an application according to Claim 17.

[0015] The present invention also provides a computer readable information storage medium according to Claim 18.

Advantageous Effects of Invention

[0016] According to the present invention, it is possible to restrict a terminal device in which content or an application can be used to a single terminal device among one authorized terminal device and one or more unauthorized terminal devices.

BRIEF DESCRIPTION OF DRAWINGS

[0017]

FIG. 1 shows an overall structure of a content or application providing system according to an embodiment of the present invention;
FIG. 2 shows one example of processing executed in the content or application providing system;
FIG. 3 shows one example of a user table;
FIG. 4 shows one example of processing executed in the content or application providing system;
FIG. 5 shows one example of data stored in an auxiliary storage
unit of a terminal device;
FIG. 6 shows one example of a terminal table;
FIG. 7 shows one example of a menu screen;
FIG. 8 is a functional block diagram of a content or application providing system according to a first embodiment;
FIG. 9 explains an example of a generation rule;
FIG. 10 shows one example of processing executed in the content or application providing system;
FIG. 11 shows one example of processing executed in the content or application providing system;
FIG. 12 shows one example of processing executed in the content or application providing system;
FIG. 13 is a functional block diagram of a content or application providing system according to a second embodiment;
FIG. 14 shows one example of generation rule information;
FIG. 15 shows another example of the generation rule information;
FIG. 16 is a functional block diagram of a content or application providing system according to a third embodiment;
FIG. 17 shows one example of update frequency information stored in a first update frequency information storage unit;
FIG. 18 shows one example of generation rule information; and
FIG. 19 shows one example of a terminal table.

DESCRIPTION OF EMBODIMENTS

[0018] In the following, examples of embodiments of the present invention will be described in detail with reference to the accompanying drawings.

[0019] [First Embodiment] FIG. 1 shows an overall structure of a content or application providing system according to a first embodiment of the present invention. As shown in FIG. 1, a content or application providing system 1 according to the first embodiment includes a terminal device 10 and a managing system 20 (an authentication system). The terminal device 10 and the managing system 20 are connected to a communication network 2 including, for example, the Internet, or the like, and can execute data communication with each other.

[0020] The managing system 20 includes one or more server computers. In the example shown in FIG. 1, the managing system 20 includes a server device 22 (an authentication device) and a database 24. The server device 22 is a device for providing content to the terminal device 10. "Content" refers to, for example, an electronic book, an image, a video, music, a game, or the like. The server device 22 executes processing based on a processing request received from the terminal device 10. For example, the server device 22 has a control unit (for example, a CPU or the like), a main memory unit (for example, a RAM or the like), an auxiliary storage unit (for example, a hard disk or a solid state drive), an optical disk drive for reading a program and data stored in an optical disk (an information storage medium), and a communication interface.

[0021] The control unit executes processing according to a program stored in the auxiliary storage unit. For example, a program and data is supplied via an optical disk (an information storage medium) to the auxiliary storage unit of the server device 22. That is, an optical disk storing a program and data is mounted in the optical disk drive, and the program and data stored in the optical disk is read by the optical disk drive to be stored in the auxiliary storage unit. Note that a program and data may be supplied to the auxiliary storage unit via an information storage medium (for example, a memory card) other than an optical disk. Further, a program and data may be supplied to the auxiliary storage unit via the communication network 2.

[0022] The server device 22 can access the database 24. In the database 24, for example, data on a user using the content or application providing system 1, data on

content provided by the content or application providing system 1, and so forth are stored. Note that the database 24 may be built in a server computer other than the server device 22 or in the server computer 22.

[0023] The terminal device 10 is an information processing device on which a user uses content or an application. The terminal device 10 is, for example, a personal computer, a portable phone, a portable information terminal, or the like. For example, the terminal device 10 has a control unit (for example, a CPU), a main memory unit (for example, a RAM), an auxiliary storage unit (for example, a hard disk or a solid state drive), an optical disk drive, an operation unit, a display unit (for example, a liquid crystal display), a sound output unit (for example, a speaker), and a communication interface.

[0024] Note that, for example, a program and data is supplied to the auxiliary storage unit of the terminal device 10 via an optical disk (an information storage medium). That is, an optical disk storing a program and data is mounted in the optical disk drive, and the program and data stored in the optical disk is read by the optical disk drive to be stored in the auxiliary storage unit. Note that a program and data may be supplied to the auxiliary storage unit via an information storage medium (for example, a memory card) other than an optical disk. Further, a program and data may be supplied to the auxiliary storage unit via the communication network 2.

[0025] In this embodiment, for example, a daemon program (for example, an HTTP daemon) is activated in the server device 22. Further, a program for accessing the server device 22 is activated in the terminal device 10. According to the program, a processing request (for example, an HTTP request) is sent from the terminal device 10 to the server device 22. Then, a processing result (for example, an HTTP response) in response to the above-described processing request is sent from the server device 22 to the terminal device 10. For example, page data written in a predetermined descriptive language (for example, web page descriptive language) is sent to the terminal device 10, and a screen based on the processing result is displayed on the display unit of the terminal device 10, based on the page data.

[0026] In the above-described content or application providing system 1, content or an application is sold. For example, content data that can be reproduced according to a predetermined program that is pre-installed in the terminal device 10 is sold. Note that application software including a program for reproducing content data and content data may be sold. Alternatively, a program for reproducing content data may be sold by itself as an application. Still alternatively, other applications (for example, an editor or the like) may be sold. Note that, in the following, for brevity of description, a case will be mainly described in which an "electronic book" that can be displayed according to a pre-installed program in the terminal device 10 is sold.

[0027] A user using the content or application providing system 1 is first required to complete user registration. FIG. 2 shows one example of processing executed for user registration.

[0028] As shown in FIG. 2, initially, the control unit of the terminal device 10 displays a user information input screen (not shown) on the display unit of the terminal device 10 (S101). The user information input screen is a screen in which a user inputs information on himself/herself. Specifically, in the user information input screen, a user inputs, for example, an ID, a password, a name, an address, credit card information, and so forth. Note that the ID of a user may be set desirably or automatically by the content or application providing system 1.

[0029] The control unit of the terminal device 10 sends the user information input in the user information input screen to the server device 22 (S102). Upon receipt of the user information in the server device 22, the control unit of the server device 22 registers the received user information in the database 24 (S103).

[0030] FIG. 3 shows one example of a user table stored in the database 24. The user table is a table for storing user information input in the user information input screen. The user table shown in FIG. 3 includes "user ID", "user password", "name", "address", and "credit card information" fields. At step S103, the control unit adds a new record to the user table. Then, the control unit registers the user information received from the terminal device 10 in the respective fields of the newly added record. The above completes user registration.

[0031] FIG. 4 explains processing executed at initial access to the server device 22 by the terminal device 10 after completion of user registration.

[0032] As shown in FIG. 4, initially, the control unit of the terminal device 10 displays a user authentication screen image (not shown) on the display unit of the terminal device 10 (S201). Note that the user authentication screen is a screen for inputting a user ID and a user password, in which a user is guided to input his/her user ID and user password. The control unit of the terminal device 10 sends the user ID and user password input in the user authentication screen to the server device 22 (S202).

[0033] Upon receipt of the user ID and user password in the server device 22, the control unit of the server device 22 determines whether or not the combination of the received user ID and user password is authentic (S203). That is, the control unit of the server device 22 determines whether or not the combination of the received user ID and user password is registered in the user table. When the combination of the received user ID and user password is registered in the user table, the server device 22 determines that the combination of the received user ID and user password is authentic.

[0034] Then, the control unit of the server device 22 sends notice information to notify of a result of determination at step S203 to the terminal device 10 (S204). Upon receipt of the notice information in the terminal device 10, the control unit of the terminal device 10 determines whether or not a determination result to the effect

that the combination of the user ID and user password is authentic has been notified (S205).

[0035] Upon notice of a determination result to the effect that the combination of the user ID and user password is authentic, the control unit of the terminal device 10 reads a terminal ID (terminal identification information) stored in advance in the auxiliary storage unit. A "terminal ID" is identification information unique to each terminal device 10. In addition, the control unit automatically generates an authentication symbol string. An "authentication symbol string" is a symbol string automatically generated by the terminal device 10 to serve as a password correlated to each terminal ID. Note that, as described above, a "symbol" refers to a symbol in a broader sense, including, for example, a character, a reference mark (a symbol in a narrower sense), and so froth. Thus, a "symbol string" includes a "character string". A "symbol string" also includes a symbol string constituted of one symbol (that is, a single symbol).

[0036] Then, the control unit of the terminal device 10 sends the user ID, the terminal ID, and the authentication symbol string to the server device 22 (S206). In addition, the control unit of the terminal device 10 stores the authentication symbol string sent to the server device 22 in the auxiliary storage unit (S207) . For example, the authentication symbol string is stored together with the terminal ID. That is, for example, data such as is shown in FIG. 5 is stored in the auxiliary storage unit of the terminal device 10.

[0037] Upon receipt of the user ID, the terminal ID, and the authentication symbol string in the server device 22, the control unit of the server device 22 registers the received user ID, terminal ID, and authentication symbol string in the database 24 (S208).

[0038] FIG. 6 shows one example of a terminal table stored in the database 24. The terminal table shown in FIG. 6 includes "user ID", "terminal ID", "authentication symbol string", and "content/application information" fields. For example, a list of IDs of content (for example, an electronic book) or applications that are authentically usable in each terminal device 10 is registered in the "content/application information" field.

[0039] At step S208, the control unit of the server device 22 newly adds a record to the terminal table. Then, the control unit registers the user ID, the terminal ID, and the authentication symbol string all received from the terminal device 10 in the respective "user ID", "terminal ID", and "authentication symbol string" fields of the newly added record.

[0040] In the terminal device 10, after storing the authentication symbol string sent to the server device 22 in the auxiliary storage unit, a menu screen is displayed on the display unit (S209) . FIG. 7 shows one example of the menu screen. In the menu screen 30 shown in FIG. 7, a link button 32 for buying an electronic book (content) and a link button 34 for reading an electronic book bought are displayed.

[0041] Upon selection of the link button 32 by a user, a purchase screen (not shown) for buying an electronic book is displayed on the display unit of the terminal device 10. For example, a list of electronic books available in the content or application providing system 1 is displayed in the purchase screen. Then, a user selects his/her desired electronic book in the electronic book list displayed in the purchase screen. Upon selection of the user' s desired electronic book, purchase processing (settlement processing) is executed, followed by downloading the electronic book to the terminal device 10. The downloaded electronic book is stored in the auxiliary storage unit of the terminal device 10. Note that when an electronic book is purchased, the ID of the purchased electronic book is additionally registered in the "content/application information" field of the terminal table.

[0042] Upon selection of the link button 34 by a user, a reading screen (not shown) for reading an electronic book is displayed on the display unit of the terminal device 10. For example, a list of the electronic books stored in the auxiliary storage unit of the terminal device 10 is displayed in the reading screen. Then, the user selects his/her desired electronic book in the electronic book list displayed in the reading screen. Upon selection of the user's desired electronic book, content of the selected electronic book is displayed. In this manner, the user can read his/her desired electronic book.

[0043] Note here that processing executed at initial access to the server device 22 by the terminal device 10 after completion of user registration is described referring to Fig. 4. At initial access to the serer device 22 by the terminal device 10, the user authentication screen is displayed so that a user is requested to input a user ID and a user password. Meanwhile, at second and thereafter accesses, on principle, the user authentication screen is not displayed. That is, a user is not requested to input a user ID and a user password as user convenience is improved. Specifically, at second and thereafter accesses, whether or not the terminal device 10 is authentic is determined based on the terminal ID and the authentication symbol string (see FIG. 5) instead of a user ID and a user password. Then, use of content or an application in that terminal device 10 is permitted, based on the result of the determination (see FIG. 10 to be described later) .

[0044] Note here that, according to a conventional content or application providing system, there has been a case in which content or an application is used in two or more terminal devices (that is, one authorized terminal device and one or more unauthorized terminal devices) even though there is only one authorized terminal device that is authentically allowed to use the content or application, as described above. On the other hand, according to the content or application providing system 1 according to this embodiment, it is possible to restrict a terminal device allowed to use content or an application to a single terminal device among one authorized terminal device and one or more unauthorized terminal devices. Below, a structure for achieving such restriction will be described.

[0045] FIG. 8 is a functional block diagram showing a functional block relevant to the present invention among those achieved in the content or application providing system 1 according to this embodiment.

[0046] As shown in FIG. 8, the content or application providing system 1 includes a first authentication symbol string storage unit 100, an authentication symbol string generation unit 102, an authentication information transmission unit 108, a notice information receiving unit 110, a permitting unit 112, and a first authentication symbol string updating unit 114. For example, the first authentication symbol string storage unit 100 is implemented using the auxiliary storage unit of the terminal device 10. A functional block other than the first authentication symbol string storage unit 100 is implemented by the control unit of the terminal device 10. That is, the control unit of the terminal device 10 executes processing according to a program, thereby functioning as a functional block other than the first authentication symbol string storage unit 100.

[0047] The content or application providing system 1 further includes a second authentication symbol string storage unit 200, an authentication information receiving unit 202, a determination unit 204, a notice information transmission unit 206, and a second authentication symbol string updating unit 208. For example, the second authentication symbol string storage unit 200 is implemented using the database 24 (or the auxiliary storage unit of the server device 22). A functional block other than the second authentication symbol string storage unit 200 is achieved by the control unit of the server device 22. That is, the control unit of the server device 22 executes processing according to a program, thereby functioning as a functional block other than the second authentication symbol string storage unit 200.

[0048] Initially, the first authentication symbol string storage unit 100 will be described. The first authentication symbol string storage unit 100 stores an authentication symbol string. For example, data such as is shown in FIG. 5 is stored in the first authentication symbol string storage unit 100.

[0049] Below, the authentication symbol string generation unit 102 will be described. According to a generation rule for generating a new authentication symbol string based on at least a part of an authentication symbol string, the authentication symbol string generation unit 102 generates a new authentication symbol string based on at least a part of the authentication symbol string stored in the first authentication symbol string storage unit 100.

[0050] For example, the authentication symbol string generation unit 102 includes an extraction unit 104. According to a generation rule, the extraction unit 104 extracts one or more symbols from the authentication symbol string stored in the first authentication symbol string storage unit 100. Then, according to the generation rule, the authentication symbol string generation unit 102 generates a new authentication symbol string based on the one or more symbols extracted by the extraction unit 104.

[0051] The generation rule in this case includes a rule in which a symbol at which position in an authentication symbol string is to be extracted, and a rule on how to generate a new authentication symbol string based on one or more symbols extracted from the authentication symbol string (see the examples (1) to (7) in FIG. 9 to be described later).

[0052] Further, for example, the authentication symbol string generation unit 102 includes a conversion unit 106. According to a generation rule, the conversion unit 106 converts at least a part of the authentication symbol string stored in the first authentication symbol string storage unit 100, to thereby obtain one or more symbols. Then, according to the generation rule, the authentication symbol string generation unit 102 generates a new authentication symbol string based on the one more symbols obtained by the conversion unit 106.

[0053] The generation rule in this case includes a rule on how to convert at least a part of an authentication symbol string, and a rule on how to generate a new authentication symbol based on the one or more symbols obtained by converting at least a part of the authentication symbol string (see the examples (4) to (7) in FIG. 9 to be described later).

[0054] Note that a "rule on how to convert at least a part of an authentication symbol string" includes at least one of the rules described below:

- rule on conversion of one symbol in an authentication symbol string into one symbol (see the example (4) to be described later);
- rule on conversion of one symbol in an authentication symbol string into a plurality of symbols (see the example (5) to be described later);
- rule on conversion of a plurality of symbols in an authentication symbol string into one symbol (see the example (6) to be described later); and
- rule on conversion of a plurality of symbols in an authentication symbol string into a plurality of symbols (see the example (7) to be described later).

[0055] For example, according to the generation rule, the authentication symbol string generation unit 102 generates a symbol string including one or more symbols based on at least a part of the authentication symbol string stored in the first authentication symbol string storage unit 100, as a new authentication symbol string. The generation rule in this case includes a rule in which one or more symbols based on at least a part of an authentication symbol string is/are to be included into which position in a new authentication symbol string (see the examples (1) to (7) in FIG. 9 to be described later).

[0056] FIG. 9 explains a specific example of the generation rule. However, the generation rule is not limited to the examples (1) to (7) shown in FIG. 9.

[0057] Initially, the example (1) will be described. The generation rule in the example (1) is a generation rule to

read that a symbol at a predetermined position (hereinafter referred to as an "extraction position") in an authentication symbol string is extracted, and that a symbol string including the extracted symbol inserted in a predetermined position (hereinafter referred to as an "insertion position") thereof is obtained as a new authentication symbol string.

[0058] In the example (1), the end position is set as the "extraction position", and the head position is set as the "insertion position" . Note that a position other than the end position may be set as the "extraction position". For example, the head position may be set as the "extraction position". Further, for example, the i^{th} position from the end (i: two or larger integer) may be set as the "extraction position". Similarly, a position other than the head position may be set as the "insertion position". For example, the end position may be set as the "insertion position". The i^{th} position from the head (i: two or larger integer) may be set as the "extraction position". The "extraction position" and the "insertion position" may be different positions from each other or the same position.

[0059] In a case where the generation rule is one in the example (1) and the authentication symbol string stored in the first authentication symbol string storage unit 100 is "ABCDE", the authentication symbol string generation unit 102 (the extraction unit 104) extracts the symbol (E) at the extraction position (the end position) in the authentication symbol string stored in the first authentication symbol string storage unit 100, and obtains an authentication symbol string (for example, "EXPT4H368B") including the extracted symbol (E) inserted in the insertion position (the head position) thereof as a new authentication symbol string.

[0060] In this case, "XPT4H368B", namely, the part of the new authentication symbol string "EXPT4H368B" other than the head character "E", is generated at random. That is, the length of the part other than the head character "E" and the symbols constituting the part other than the character "E" are determined at random.

[0061] Below, the examples (2) and (3) will be described. The generation rule in the examples (2) and (3) is a generation rule to read that a plurality of symbols at predetermined extraction positions in an authentication symbol string are extracted, and that a symbol string including the plurality of extracted symbols inserted in predetermined insertion positions thereof is obtained as a new authentication symbol string.

[0062] In the example (2), the second position from the end and the end position are set as "extraction positions". In the example (3), a plurality of discrete positions are set as "extraction positions" . That is, the third position from the end and the end position are set as "extraction positions". Note that any other position may be set as the "extraction position". Further, in the examples (2) and (3), the head position and the second position from the head are set as the "insertion positions". Note that any other position may be set as the "insertion position". A plurality of discrete positions may be set as the "insertion positions".

[0063] In a case where the generation rule is one in the example (2) and the authentication symbol string stored in the first authentication symbol string storage unit 100 is "ABCDE", the authentication symbol string generation unit 102 (the extraction unit 104) extracts the symbols (DE) at the extraction positions (the second position from the end and the end position) in the authentication symbol string stored in the first authentication symbol string storage unit 100, and obtains an authentication symbol string (for example, "DEXPT4H368B") including the extracted symbols (DE) inserted in the insertion positions (the head position and the second position from the head) thereof as a new authentication symbol string. Note that in this case as well, the part "XPT4H368B" is generated at random.

[0064] In a case where the generation rule is one in the example (3), and the authentication symbol string stored in the first authentication symbol string storage unit 100 is "ABCDE", the authentication symbol string generation unit 102 (the extraction unit 104) extracts symbols (CE) at the extraction positions (the third position from the end and the end position) in the authentication symbol string stored in the first authentication symbol string storage unit 100, and obtains an authentication symbol string (for example, "CEXPT4H368B") including the extracted symbols (CE) inserted in the insertion positions (the head position and the second position from the head) thereof as a new authentication symbol string. Note that in this case as well, the part "XPT4H368B" is generated at random.

[0065] Below, the example (4) will be described. The generation rule in the example (4) is a generation rule to read that a symbol at a predetermined extraction position in an authentication symbol string is extracted, and that a symbol string including a symbol, which is obtained by converting the extracted symbol and is inserted in a predetermined insertion position thereof, is obtained as a new authentication symbol string. In the example (4), similar to the example (1), the end position is set as the "extraction position", and the head position is set as the "insertion position". Similar to the example (1), any position other than the end position may be set as the "extraction position", and any position other than the head position may be set as the "insertion position".

[0066] In a case where the generation rule is one in the example (4), and the authentication symbol string stored in the first authentication symbol string storage unit 100 is "ABCDE", the authentication symbol string generation unit 102 (the extraction unit 104) extracts the symbol (E) at the extraction position (the end position) in the authentication symbol string stored in the first authentication symbol string storage unit 100.

[0067] Then, the authentication symbol string generation unit 102 (the conversion unit 106) converts the extracted symbol (E) into another symbol according to a predetermined conversion rule. For example, the authentication symbol string generation unit 102 (the conversion

unit 106) converts the extracted symbol into another symbol according to an order predetermined with respect to the symbols. For example, the authentication symbol string generation unit 102 (the conversion unit 106) converts the extracted symbol into a symbol immediately after that symbol. Specifically, in the example (4), the extracted alphabet "E" is converted into an alphabet immediately after the alphabet "E", namely, the alphabet "F". Note that a conversion table for correlating an original symbol in conversion and a converted symbol may be stored in advance in the auxiliary storage unit, so that the conversion is executed based on the conversion table.

[0068] The authentication symbol string generation unit 102 obtains a symbol string (for example, "FXPT4H368B") including the symbol obtained through conversion inserted in the insertion position (the head position) thereof as a new symbol string. Note that the part "XPT4H368B" is generated at random in this case as well.

[0069] Below, the example (5) will be described. The generation rule in the example (5) is a generation rule to read that one symbol at a predetermined extraction position in an authentication symbol string is extracted, and that a symbol string including a plurality of symbols, which are obtained by converting the one extracted symbol and are inserted in an insertion position thereof, is obtained as a new authentication symbol string.

[0070] In the example (5), similar to the example (1), the end position is set as the "extraction position". Further, similar to the examples (2) and (3), the head position and the second position from the head are set as the "insertion positions". Similar to the examples (1) to (3), any other position may be set as the "extraction position" or the "insertion position".

[0071] In a case where the generation rule is one in the example (5) and the authentication symbol string stored in the first authentication symbol string storage unit 100 is "ABCDE", the authentication symbol string generation unit 102 (the extraction unit 104) extracts the symbol (E) at the extraction position (the end position) in the authentication symbol string stored in the first authentication symbol string storage unit 100.

[0072] Then, the authentication symbol string generation unit 102 (the conversion unit 106) converts the one extracted symbol (E) into a plurality of symbols according to a predetermined conversion rule. For example, the authentication symbol string generation unit 102 (the conversion unit 106) converts the one extracted symbol into a plurality of symbols according to an order predetermined with respect to the symbols. For example, the authentication symbol string generation unit 102 (the conversion unit 106) converts the extracted symbol into two symbols immediately after the extracted symbol. Specifically, in the example (5), the alphabet "E" is converted into two alphabets, namely, the alphabets "FG", immediately after that alphabet "E". Note that a conversion table for correlating an original symbol in conversion and converted symbols may be stored in advance in the auxiliary storage unit, so that the conversion is executed based on the conversion table.

[0073] Then, the authentication symbol string generation unit 102 obtains a symbol string (for example "FGXPT4H368B") including the plurality of symbols, which are obtained through conversion and are inserted in the insertion position (the head position and the second position from the head) thereof, as a new symbol string. Note that the part "XPT4H368B" is generated at random in this case as well.

[0074] Below, the example (6) will be described. The generation rule in the example (6) is a generation rule to read that a plurality of symbols at predetermined extraction positions in an authentication symbol string are extracted, and that a symbol string including one symbol, which is obtained by converting the plurality of extracted symbols and is inserted in a predetermined insertion position thereof, is obtained as a new authentication symbol string.

[0075] In the example (6), similar to the example (2), the second position from the end and the end position are set as the "extraction positions". Similar to the example (1), the head position is set as the "insertion position". Note that similar to the examples (1) and (2), any other position may be set as the "extraction position" or the "insertion position".

[0076] In a case where the generation rule is one in the example (6), and the authentication symbol string stored in the first authentication symbol string storage unit 100 is "ABCDE", the authentication symbol string generation unit 102 (the extraction unit 104) extracts a plurality of symbols (DE) at the extraction positions (the second position from the end and the end position) in the authentication symbol string stored in the first authentication symbol string storage unit 100.

[0077] Then, the authentication symbol string generation unit 102 (the conversion unit 106) converts the plurality of extracted symbols (DE) into a single symbol according to a predetermined conversion rule. For example, in this case, a conversion table for correlating a plurality of original symbols in conversion and one converted symbol is stored in advance in the auxiliary storage unit, so that the authentication symbol string generation unit 102 (the conversion unit 106) executes the conversion based on the conversion table. In the example (6), the plurality of extracted characters "DE" are converted into the character "K".

[0078] Then, the authentication symbol string generation unit 102 obtains a symbol string (for example "KXPT4H368B") including the single symbol, which is obtained through conversion and is inserted in the insertion position (the head position) thereof, as a new symbol string. Note that the part "XPT4H368B" is generated at random in this case as well.

[0079] Below, the example (7) will be described. The generation rule in the example (7) is a generation rule to read that a plurality of symbols at predetermined extrac-

tion positions in an authentication symbol string are extracted, and that a symbol string including a plurality of symbols, which are obtained by converting the plurality of extracted symbols and are inserted in predetermined insertion positions thereof, is obtained as a new authentication symbol string.

[0080] In the example (7), similar to the example (2), the second position from the end and the end position are set as "extraction positions". Moreover, the head position, the second position from the head and the third position from the head are set as the "insertion positions". Note that any other position may be set as the "extraction position" or the "insertion position".

[0081] In a case where the generation rule is one in the example (7) and the authentication symbol string stored in the first authentication symbol string storage unit 100 is "ABCDE", the authentication symbol string generation unit 102 (the extraction unit 104) extracts a plurality of symbols (DE) at the extraction positions (the second position from the end and the end position) in the authentication symbol string stored in the first authentication symbol string storage unit 100.

[0082] Then, the authentication symbol string generation unit 102 (the conversion unit 106) converts the plurality of extracted symbols (DE) into a plurality of symbols according to a predetermined conversion rule. In this case, the m (m: two or larger integer) number of extracted symbols are converted into the n (n: two or larger integer) number of symbols. Note that "m" and "n" may be the same or different numeric value.

[0083] For example, in this case, a conversion table for correlating a plurality of original symbols in conversion and a plurality of converted symbols may be stored in advance in the auxiliary storage unit, so that the authentication symbol string generation unit 102 (the conversion unit 106) executes the conversion based on the conversion table. In the example (7), the plurality of extracted characters "DE" are converted into a plurality of characters "MLS" .

[0084] Then, the authentication symbol string generation unit 102 (the conversion unit 106) obtains a symbol string (for example, "MLSXPT4H368B") including the plurality of converted symbols inserted in the insertion position (the head position) thereof as a new symbol string. Note that the part "XPT4H368B" is generated at random in this case as well.

[0085] Below, the authentication information transmission unit 108 and the authentication information receiving unit 202 will be described. The authentication information transmission unit 108 sends the terminal ID (terminal identification information) of the terminal device 10 and an authentication symbol string (a new authentication symbol string) generated by the authentication symbol string generation unit 102 to the server device 22. Thereafter, the authentication information receiving unit 202 receives the terminal ID and the authentication symbol string (a new authentication symbol string) both sent from the authentication information transmission unit 108.

[0086] Below, the second authentication symbol string storage unit 200 will be described. The second authentication symbol string storage unit 200 stores an authentication symbol string so as to be correlated to a terminal ID. For example, a terminal table such as is shown in FIG. 6 is stored in the second authentication symbol string storage unit 200. Note that, on principle, in the second authentication symbol string storage unit 200 (terminal table), an authentication symbol string same as the authentication symbol string stored in the auxiliary storage unit of the terminal device 10 is stored so as to be correlated to the terminal ID of the terminal device 10. That is, for example, an authentication symbol string (ABCDE) stored in the auxiliary storage unit of the terminal device 10 having the terminal ID "T00001" is stored in the second authentication symbol string storage unit 200 (terminal table) so as to be correlated to the terminal ID "T00001".

[0087] Below, the determination unit 204 will be described. The determination unit 204 determines whether or not the terminal ID and authentication symbol string received by the authentication information receiving unit 202 are authentic.

[0088] Specifically, the determination unit 204 determines whether or not the authentication symbol string received by the authentication information receiving unit 202 belongs to a type of "an authentication symbol string that can be generated based on at least a part of the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202, according to the generation rule same as that which is used in the authentication symbol string generation unit 102".

[0089] In order to determine whether or not the authentication symbol string received by the authentication information receiving unit 202 belongs to the above mentioned type, the determination unit 204 determines whether or not the authentication symbol string received by the authentication information receiving unit 202 has a characteristic feature which an authentication symbol string belonging to the above mentioned type should have. In other words, the determination unit 204 determines whether or not the authentication symbol string received by the authentication information receiving unit 202 satisfies a condition which an authentication symbol string belonging to the above mentioned type should satisfy.

[0090] For example, in a case where the generation rule is one in the example (1) in FIG. 9, a characteristic feature which an authentication symbol string belonging to the above mentioned type should have is that "the symbol (character) at the head is the same as the symbol (character) at the end of the authentication symbol string stored in the second authentication symbol string storage unit 200". Therefore, the above mentioned "condition" is to read that "the symbol (character) at the head of the authentication symbol string received by the authentica-

tion information receiving unit 202 is the same as the symbol (character) at the end of the authentication symbol string stored in the second authentication symbol string storage unit 200".

[0091] For example, in a case where the generation rule is one in the example (4) in FIG. 9, a characteristic feature which an authentication symbol string belonging to the above mentioned type should have is that "the symbol (character) at the head is a symbol (character) obtained by converting the symbol (character) at the end of the authentication symbol string stored in the second authentication symbol string storage unit 200 according to a predetermined conversion rule". Therefore, the above mentioned "condition" is to read that "the symbol (character) at the head of the authentication symbol string received by the authentication information receiving unit 202 is a symbol (character) obtained by converting the symbol (character) at the end of the authentication symbol string stored in the second authentication symbol string storage unit 200 according to a predetermined conversion rule".

[0092] Upon determination that the authentication symbol string received by the authentication information receiving unit 202 belongs to the above mentioned type, the determination unit 204 determines that the terminal ID and authentication symbol string received by the authentication information receiving unit 202 are authentic.

[0093] Blow, the notice information transmission unit 206 and the notice information receiving unit 110 will be described. Upon determination that the terminal ID and authentication symbol string received by the authentication information receiving unit 202 are authentic, the notice information transmission unit 206 sends notice information to the terminal device 10 to notify that the terminal ID and authentication symbol string received by the authentication information receiving unit 202 are authentic and/or that use of content or an application in the terminal device 10 is permitted. Thereafter, the notice information receiving unit 110 receives the notice information sent from the notice information transmission unit 206.

[0094] Below, the permitting unit 112 will be described. The permitting unit 112 permits use of content or an application, based on the notice information received by the notice information receiving unit 110. In the terminal device 10, upon determination that the terminal ID and authentication symbol string received by the authentication information receiving unit 202 are authentic, it is permitted to output content, such as music, image, video, electronic book, or the like, and to execute content, such as a game or the like, or an application.

[0095] Below, the first authentication symbol string updating unit 114 and the second authentication symbol string updating unit 208 will be described.

[0096] When the determination unit 204 determines that the terminal ID and authentication symbol string received by the authentication information receiving unit 202 are authentic, the second authentication symbol string updating unit 208 updates the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202 to the authentication symbol string received by the authentication information receiving unit 202.

[0097] Further, when the determination unit 204 determines that the terminal ID and authentication symbol string received by the authentication information receiving unit 202 are authentic, the first authentication symbol string updating unit 114 updates the authentication symbol string stored in the first authentication symbol string storage unit 100 to the authentication symbol string sent by the authentication information transmission unit 108.

[0098] With the above described operation of the first authentication symbol string updating unit 114 and the second authentication symbol string updating unit 208, the authentication symbol string stored in the first authentication symbol string storage unit 100 of the terminal device 10 and the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID of the terminal device 10 are updated to the same authentication symbol string, when the determination unit 204 determines that the terminal ID and authentication symbol string received by the authentication information receiving unit 202 are authentic.

[0099] Below, processing executed in implementing the above described functional blocks will be described. FIG. 10 shows processing executed at second and thereafter accesses from the terminal device 10 to the server device 22. The control unit of the terminal device 10 executes the processing shown in FIG. 10 according to the program, thereby functioning as the authentication symbol string generation unit 102, the authentication information transmission unit 108, the notice information receiving unit 110, the permitting unit 112, and the first authentication symbol string updating unit 114. Meanwhile, the control unit of the server device 22 executes the processing shown in FIG. 10 according to the program, thereby functioning as the authentication information receiving unit 202, the determination unit 204, the notice information transmission unit 206, and the second authentication symbol string updating unit 208.

[0100] As shown in FIG. 10, initially, according to a predetermined generation rule, the control unit (the authentication symbol string generation unit 102) of the terminal device 10 generates a new authentication symbol string, based on the authentication symbol string stored in the auxiliary storage unit (the first authentication symbol string storage unit 100) of the terminal device 10 (S301). Specifically, a new authentication symbol string is generated according to, for example, a generation rule such as is described referring to FIG. 9. Thereafter, the control unit (the authentication information transmission unit 108) of the terminal device 10 sends the terminal ID and the new authentication symbol string generated at step S301 to the server device 22 (S302).

[0101] Upon receipt of the terminal ID and the authentication symbol string by the server device 22, the control unit of the server device 22 accesses the terminal table (the second authentication symbol string storage unit 200), and obtains the authentication symbol string stored so as to be correlated to the received terminal ID (S303).

[0102] Then, the control unit (the determination unit 204) of the server device 22 determines whether or not the combination of the received terminal ID and authentication symbol string is authentic (S304) . Specifically, the control unit determines whether or not the received authentication symbol string corresponds to "an authentication symbol string that can be generated based on at least a part of the authentication symbol string obtained at step S303, according to a generation rule". Note that the "generation rule" at step S304 is the generation rule same as that which is used in generation of a new authentication symbol string at step S301.

[0103] For example, in the auxiliary storage unit of the server device 22, a condition in which "an authentication symbol string that can be generated based on at least a part of the authentication symbol string obtained at step S303, according to the generation rule" should satisfy is stored in advance. As described above, for example, in a case where the generation rule is one in the example (1) in FIG. 9, the stored condition should be read as that "the symbol (character) at the head of the authentication symbol string received by the authentication information receiving unit 202 is the same as the symbol (character) at the end of the authentication symbol string stored in the second authentication symbol string storage unit 200". Then, at step S304, the control unit of the server device 22 determines whether or not the received authentication symbol string satisfies the condition. When the received authentication symbol string satisfies the condition, it is determined that the received authentication symbol string corresponds to "an authentication symbol string that can be generated based on at least a part of the authentication symbol string obtained at step S303, according to the generation rule".

[0104] After the processing at step S304 executed, the control unit (the notice information transmission unit 206) of the server device 22 sends information to the terminal device 10 to notify the terminal device 10 of the result of the determination at step S304 (S305) .

[0105] Note that upon determination at step S304 that the combination of the terminal ID and the authentication symbol string is authentic, the control unit further sends information to the terminal device 10 to notify of a list of content (for example, an electronic book) usable in the terminal device 10. That is, the control unit reads from the terminal table, a list of content IDs stored so as to be correlated to the terminal ID received from the terminal device 10, and sends the list to the terminal device 10.

[0106] Upon receipt of the notice information by the terminal device 10, the control unit of the terminal device 10 determines whether or not a result of determination to the effect that the terminal ID and authentication symbol string are authentic is notified from the server device 22 (S306).

[0107] Upon notice from the server device 22, of a result of determination to the effect that the terminal ID and the authentication symbol string are authentic, the control unit of the terminal device 10 (the first authentication symbol string updating unit 114) updates the authentication symbol string stored in the auxiliary storage unit (the first authentication symbol string storage unit 100) of the terminal device 10 to the authentication symbol string sent to the server device 22 at step S302 (that is, the authentication symbol string generated at step S301) (S307).

[0108] Further, the control unit (the permitting unit 112) of the terminal device 10 displays a menu screen (FIG. 7) on the display unit (S308), and permits use of content (an electronic book) stored in the terminal device 10. That is, use of content is permitted, based on the list of content usable in the terminal device 10, notified by the server device 22. That is, a user can reproduce and/or execute the content.

[0109] On the other hand, in the server device 22, after the processing at step S305 executed, it is determined whether or not a result of determination to the effect that the terminal ID and the authentication symbol string are authentic is obtained at step S304 (S309) . In a case where a result of determination to the effect that the terminal ID and the authentication symbol string are authentic is obtained at step S304, the control unit (the second authentication symbol string updating unit 208) of the server device 22 accesses the terminal table (the second authentication symbol string storage unit 200), and updates the authentication symbol string stored so as to be correlated to the terminal ID received at step S302 to the authentication symbol string received at step S302 (S310). Description on the processing shown in FIG. 10 is completed with the above.

[0110] According to the above described content or application providing system 1 according to the first embodiment, it is possible to restrict a terminal device in which content or an application can be used to a single terminal device among a single authorized terminal device and one or more unauthorized terminal devices.

[0111] Below, assume a situation in which content or an application stored in the terminal device 10 (an authorized terminal device) authentically allowed to use the content or application is copied to one or more other terminal devices 10 (one or more unauthorized terminal devices), and the terminal ID and the authentication symbol string stored in the authorized terminal device are registered (impersonation) in these unauthorized terminal devices as a terminal ID and an authentication symbol string thereof. That is, assume a situation in which the terminal ID, the authentication symbol string, and the content stored in the authorized terminal device are stored also in a plurality of terminal devices 10 (the authorized terminal device and one or more unauthorized terminal devices).

[0112] When any terminal device 10 (that is, any of the

authorized terminal device and the one or more unauthorized terminal devices) accesses the server device 22 in the above described situation, the terminal ID and authentication symbol string of the authorized terminal device are sent to the server device 22, and therefore content can be used in the terminal device 10.

[0113] In the above, the authentication symbol string stored in the terminal device 10 and the authentication symbol string stored in the server device 22 so as to be correlated to the terminal ID of the authorized terminal device are updated. Thus, even though another terminal device 10 thereafter accesses the server device 22, it is determined that the combination of the terminal ID and the authentication symbol string is not authentic, and therefore the content cannot be used in that terminal device 10.

[0114] As describe above, according to the content or application providing system 1, even though an terminal ID, an authentication symbol string, and content or an application stored in one authorized terminal device are stored in a plurality of terminal devices 10 as well (the one authorized terminal device and one or more unauthorized terminal devices), it is possible to restrict a terminal device in which content or an application can be used to one terminal device among these plurality of terminal devices 10.

[0115] Note here that there may be caused a case, due to deficiency or the like caused to the communication network 2, in which the authentication symbol string stored in the terminal device 10 (the first authentication symbol string storage unit 100) does not coincide with that stored in the server device 22 (the second authentication symbol string storage unit 200). For example, if any deficiency should be caused to the communication network 2 in exchanging notice information at step S305 in FIG. 10, a situation may be resulted in which only the authentication symbol string stored in the server device 22 is updated while that stored in the terminal device 10 remains not updated.

[0116] In such a case, as the authentication symbol string stored in the terminal device 10 does not coincide with that stored in the server device 22, it will be determined at step S304 in FIG. 10 at the next access from the terminal device 10 to the server device 22 that the combination of the terminal ID and the authentication symbol string is not authentic. As a result, it will be determined at step S306 that a result of determination to the effect that the terminal ID and the authentication symbol string are authentic is not notified by the server device 22, and therefore a user will not be allowed to use content or an application.

[0117] Regarding this point, according to the content or application providing system 1, in a case where it is determined at S306 in FIG. 10 that a result of determination to the effect that the terminal ID and the authentication symbol string are authentic is not notified by the server device 22, the processing shown in FIG. 11 is executed. As a result, it is possible to ensure that an authentic user can use content or an application.

[0118] When it is determined at step S306 in FIG. 10 that a result of determination to the effect that the terminal ID and the authentication symbol string are authentic is not notified by the server device 22, the control unit of the terminal device 10 displays a user authentication screen on the display unit (S401), as shown in FIG. 11. The user authentication screen is the same as that displayed at step S201 in FIG. 4.

[0119] The control unit of the terminal device 10 sends the user ID and user password both input in the user authentication screen and the terminal ID stored in the auxiliary storage unit to the server device 22 (S402) . Upon receipt of the user ID, the user password, and the terminal ID by the server device 22, the control unit of the server device 22 determines whether or not the combination of the received user ID and user password is authentic (S403). The processing at step S403 is the same as that at step S203 in FIG. 4.

[0120] Upon determination that the combination of the user ID and the user password is authentic, the control unit of the server device 22 determines whether or not the combination of the user ID and terminal ID both received at step S402 is authentic (S404) . That is, the control unit determines whether or not the combination of the user ID and terminal ID both received at S402 is registered in the terminal table.

[0121] Upon determination that the combination of the user ID and the terminal ID is authentic, the control unit of the server device 22 accesses the terminal table, and obtains the authentication symbol string stored so as to be correlated to the terminal ID received at step S402 (S405). Then, the control unit sends the authentication symbol string to the terminal device 10 (S406). Note that in a case where it is not determined at step S403 that the combination of the user ID and the user password is authentic, and at step S404 that the combination of the user ID and the terminal ID is authentic, the processing at steps S405 and S406 is not executed.

[0122] Upon receipt of the authentication symbol string sent from the server device 22 by the terminal device 10, the control unit of the terminal device 10 updates the authentication symbol string stored in the auxiliary storage unit to the received authentication symbol string (S407). Then, the control unit executes the processing at step S301 in FIG. 10. In this case, as the authentication symbol string stored in the terminal device 10 and that stored in the server device 22 coincide with each other, a user can use content (an electronic book).

[0123] According to the above described processing shown in FIG. 11, even when a situation is resulted, due to deficiency or the like caused to the communication network 2, in which the authentication symbol string stored in the terminal device 10 does not coincide with that stored in the server device 22, an authentic user can initialize the authentication symbol string stored in the terminal device 10 and that in the server device 22 to the same authentication symbol string. As a result, it is pos-

sible to ensure that an authentic user can use content or an application.

[0124] Note that, in the processing shown in FIG. 11, the authentication symbol string stored in the terminal device 10 is updated to the authentication symbol string stored in the server device 22, to thereby initialize the situation so that the authentication symbol string stored in the terminal device 10 and that stored in the server device 22 coincide with each other. However, the authentication symbol string stored in the server device 22 may be updated to that stored in the terminal device 10, to thereby initialize the situation so that the authentication symbol string stored in the terminal device 10 and that stored in the server device 22 coincide with each other. FIG. 12 shows one example of processing in that case.

[0125] The processing at S501 and S502 in FIG. 12 is similar to the processing at S401 and S402 in FIG. 11. Upon receipt of the user ID, user password, and terminal ID sent from the terminal device 10 by the server device 22, the control unit of the server device 22 determines whether or not the combination of the user ID and the user password sent from the terminal device 10 is authentic (S503). Further, the control unit of the server device 22 determines whether or not the combination of the user ID and the terminal ID sent from the terminal device 10 is authentic (S504). The processing at steps S503 and S504 is similar to the processing at steps S403 and S404 in FIG. 11.

[0126] The control unit of the server device 22 sends information to the terminal device 10 to notify the terminal device 10 of a result of the determination at steps S503 and S504 (S505). Upon receipt of the above-described notice information by the terminal device 10, the control unit of the terminal device 10 determines whether or not a result of determination to the effect that the combination of the user ID and the user password is authentic and that the combination of the user ID and the terminal ID is also authentic is notified (S506) . When it is determined that a result of determination to the effect that the combination of the user ID and the user password is authentic and the combination of the user ID and the terminal ID is authentic as well is notified, the control unit of the terminal device 10 obtains the authentication symbol string stored in the auxiliary storage unit (S507), and sends the authentication symbol string to the server device 22 together with the terminal ID (S508).

[0127] Upon receipt of the terminal ID and the authentication symbol string by the server device 22, the control unit of the server device 22 accesses the terminal table, and updates the authentication symbol string stored so as to be correlated to the received terminal ID to the received authentication symbol string (S509).

[0128] With the processing shown in FIG. 12 as well, similar to the processing in FIG. 11, even though a situation is resulted, due to deficiency or the like caused to the communication network 2, in which the authentication symbol string stored in the terminal device 10 and that stored in the server device 22 do not coincide with each other, an authentic user can initialize the situation so that the authentication symbol string stored in the terminal device 10 and that stored in the server device 22 coincide with each other. As a result, it is possible to ensure that an authentic user can use content or an application.

[0129] [Second Embodiment] A content or application providing system according to a second embodiment of the present invention will be described. An overall structure of the content or application providing system 1 according to the second embodiment is similar to that in the first embodiment. In the following, as to the content or application providing system 1 according to the second embodiment, a difference from the first embodiment will be described.

[0130] In the content or application providing system 1 according to the second embodiment, the generation rule for generating a new authentication symbol string is changed depending on an original authentication symbol string for generation. In the following, a structure for implementing such a function will be described.

[0131] FIG. 13 is a functional block diagram showing a functional block relevant to the present invention among those which are implemented in the content or application providing system 1 according to the second embodiment.

[0132] The content or application providing system 1 according to the second embodiment differs from the first embodiment in that the former includes a first generation rule information storage unit 116 and a second generation rule information storage unit 210. For example, the first generation rule information storage unit 116 is implemented using the auxiliary storage unit of the terminal device 10, and the second generation rule information storage unit 210 is implemented using the auxiliary storage unit of the server device 22 (or the database 24).

[0133] The first generation rule information storage unit 116 stores generation rule information. Generation rule information is information for correlating information on an authentication symbol string and a generation rule for generating a new authentication symbol string based on an authentication symbol string.

[0134] "Information on an authentication symbol string" refers to information concerning, for example, the length of an authentication symbol string. FIG. 14 shows one example of the generation rule information in a case where the "information on an authentication symbol string" is information on the length of an authentication symbol string. In the generation rule information shown in FIG. 14, a generation rule for an authentication symbol string is correlated to a range of the length of an authentication symbol string. In FIG. 14, "Xa" refers to a predetermined value indicating the length (the number of characters) of an authentication symbol string, and a "generation rule A" and a "generation rule B" are different generation rules.

[0135] For example, the generation rules A and B are each "a generation rule for extracting one or more symbols at one or more extraction positions in an authenti-

cation symbol string, and generating a symbol string including the extracted one or more symbols inserted in one or more insertion positions thereof as a new authentication symbol string" (see the examples (1) to (3) in FIG. 9) . The generation rules A and B are different from each other in at least one of the above-mentioned "extraction position" and "insertion position".

[0136] Specifically, for example, the generation rule A is the generation rule in the example (1) in FIG. 9, for generating a new authentication symbol string by extracting a symbol at the end position in an authentication symbol string. Meanwhile, the generation rule B is a generation rule similar to that in the example (1) in FIG. 9 but different from the generation rule A in that a symbol at the head position in an authentication symbol string is extracted.

[0137] Alternatively, for example, the generation rule A is the generation rule in the example (1) in FIG. 9, for generating a symbol string including an extracted symbol inserted in the head position thereof as a new authentication symbol string. Meanwhile, the generation rule B is a generation rule similar to that in the example (1) in FIG. 9 but different from the generation rule A in that a symbol string including an extracted symbol inserted in the end position thereof is generated as a new authentication symbol string.

[0138] Further, for example, the generation rules A and B are each "a generation rule for extracting one or more symbols at one or more extraction positions in an authentication symbol string, and generating a symbol string including one or more symbols, which are obtained by converting the one or more extracted symbols according to a conversion rule and are inserted in one or more insertion positions thereof, as a new authentication symbol string" (see the examples (4) to (7) in FIG. 9). The generation rules A and B are different from each other in the "conversion rule".

[0139] Specifically, for example, the generation rule A is the generation rule in the example (4) in FIG. 9, while the generation rule B is the generation rule in the example (5) in FIG. 9. Alternatively, the generation rule A is the generation rule in the example (6) in FIG. 9, while the generation rule B is the generation rule in the example (7) in FIG. 9.

[0140] Note that the generation rules A, B are not limited to the above-described examples. For example, the generation rule A may be the generation rule in the example (1) in FIG. 9, while the generation rule B may be the generation rule in the example (2) in FIG. 9.

[0141] Further, "information on an authentication symbol string" refers to information concerning, for example, the type of a symbol at a predetermined position in an authentication symbol string. Note here that a "predetermined position" is, for example, the "head position" or the "end position". The "predetermined position" may be a position other than the "head position" and the "end position" . FIG. 15 shows one example of the generation rule information in a case where the "information on an authentication symbol string" is information on the type of a symbol at a predetermined position in an authentication symbol string. In the generation rule information shown in FIG. 15, the type of a symbol is correlated to a generation rule of an authentication symbol string. In FIG. 15, the "symbol group A" is a group to which certain symbols belong, while the "symbol group B" is a group to which other symbols belong. The "generation rule A" and the "generation rule B" are similar to those in FIG. 14.

[0142] The second generation rule information storage unit 210 stores the generation rule information stored in the first generation rule information storage unit 116.

[0143] The authentication symbol string generation unit 102 specifies a generation rule corresponding to the authentication symbol string stored in the first authentication symbol string storage unit 100, based on the generation rule information stored in the first generation rule information storage unit 116. Then, according to that generation rule, the authentication symbol string generation unit 102 generates a new authentication symbol string based on at least a part of the authentication symbol string stored in the first authentication symbol string storage unit 100.

[0144] For example, if generation rule information such as is shown in FIG. 14 is stored in the first generation rule information storage unit 116, the authentication symbol string generation unit 102 uses a generation rule correlated to the length of the authentication symbol string stored in the first authentication symbol string storage unit 100. For example, when the length (x) of the authentication symbol string stored in the first authentication symbol string storage unit 100 satisfies "x<Xa", the authentication symbol string generation unit 102 uses the generation rule A. That is, according to the generation rule A, the authentication symbol string generation unit 102 generates a new authentication symbol string based on at least a part of the authentication symbol string stored in the first authentication symbol string storage unit 100.

[0145] Meanwhile, for example, if generation rule information such as is shown in FIG. 15 is stored in the first generation rule information storage unit 116, the authentication symbol string generation unit 102 uses a generation rule correlated to the type of a symbol at a predetermined position (for example, at the head position) in the authentication symbol string stored in the first authentication symbol string storage unit 100. For example, when the symbol at a predetermined position (for example, at the head position) in the authentication symbol string stored in the first authentication symbol string storage unit 100 belongs to the group A, the authentication symbol string generation unit 102 uses the generation rule A.

[0146] The determination unit 204 specifies a generation rule corresponding to the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit

202, based on the generation rule information stored in the second generation rule information storage unit 210. Then, the determination unit 204 determines whether or not the authentication symbol string received by the authentication information receiving unit 202 belongs to the type of "an authentication symbol string that can be generated based on at least a part of the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202, according to the specified generation rule".

[0147] For example, if generation rule information such as is shown in FIG. 14 is stored in the second generation rule information storage unit 210, the determination unit 204 determines whether or not the authentication symbol string received by the authentication information receiving unit 202 belongs to the type of "an authentication symbol string that can be generated based on at least a part of the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202, according to the generation rule correlated to the length of the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202".

[0148] For example, when the length (x) of the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202 satisfies "x<Xa", the determination unit 204 determines whether or not the authentication symbol string received by the authentication information receiving unit 202 belongs to the type of "an authentication symbol string that can be generated based on at least a part of the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202, according to the generation rule A".

[0149] Meanwhile, for example, if generation rule information such as is shown in FIG. 15 is stored in the second generation rule information storage unit 210, the determination unit 204 determines whether or not the authentication symbol string received by the authentication information receiving unit 202 belongs to the type of "an authentication symbol string that can be generated based on at least a part of the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202, according to the generation rule correlated to the type of a symbol at a predetermined position in the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202".

[0150] For example, when the symbol at a predetermined position in the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202 belongs to the symbol group A, the determination unit 204 determines whether or not the authentication symbol string received by the authentication information receiving unit 202 belongs to the type of "an authentication symbol string that can be generated based on at least a part of the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202, according to the generation rule A".

[0151] Note that the functional blocks other than the first generation rule information storage unit 116, the second generation rule information storage unit 210, the authentication symbol string generation unit 102, and the determination unit 204 are similar to those in the first embodiment.

[0152] Below, processing executed in the content or application providing system 1 according to the second embodiment will be described. In the content or application providing system 1 according to the second embodiment as well, processing similar to those shown in FIGs 2, 4, 10, and 11 (or FIG. 12) is executed.

[0153] However, at step S301 in FIG. 10, the control unit of the terminal device 10 specifies a generation rule correlated to the authentication symbol string stored in the auxiliary storage unit of the terminal device 10, based on the generation rule information stored in the storage unit of the terminal device 10, and uses the generation rule specified. When generation rule information such as is shown in FIG. 14 is stored, the control unit uses the generation rule correlated to the length of the authentication symbol string stored in the auxiliary storage unit. Meanwhile, for example, when generation rule information such as is shown in FIG. 15 is stored, the control unit uses the generation rule correlated to the type of a symbol at a predetermined position in the authentication symbol string stored in the auxiliary storage unit.

[0154] Further, at step S304 in FIG. 10, the control unit of the server device 22 specifies a generation rule correlated to the authentication symbol string obtained at step S303, based on the generation rule information stored in the auxiliary storage unit of the server device 22 (or the database 24). Then, the control unit determines whether or not the authentication symbol string received at step S302 corresponds to "an authentication symbol string that can be generated based on at least a part of the authentication symbol string obtained at step S303, according to the specified generation rule".

[0155] For example, when generation rule information such as is shown in FIG. 14 is stored, the control unit determines whether or not the authentication symbol string received at step S302 corresponds to "an authen-

tication symbol string that can be generated based on the authentication symbol string obtained at step S303, according to the generation rule correlated to the length of the authentication symbol string obtained at step S303".

[0156] Further, for example, when generation rule information such as is shown in FIG. 15 is stored, the control unit determines whether or not the authentication symbol string received at step S302 corresponds to "an authentication symbol string that can be generated based on the authentication symbol string obtained at step S303, according to the generation rule correlated to the type of a symbol at a predetermined position in the authentication symbol string obtained at step S303".

[0157] According to the content or application providing system 1 according to the second embodiment described above, it is possible to change the generation rule for generating a new authentication symbol string. According to the content or application providing system 1 according to the second embodiment, it is possible to enhance difficulty in prediction of an authentication symbol string. That is, according to the content or application providing system 1 according to the second embodiment, it is possible to make it more difficult for a person trying to illegally use content or an application to predict an authentication symbol string.

[0158] [Third Embodiment] A content or application providing system according to a third embodiment of the present invention will be described. An overall structure of a content or application providing system 1 according to the third embodiment is similar to that in the first embodiment. In the following, as to a content or application providing system 1 according to the third embodiment, a difference from the first embodiment will be described.

[0159] A content or application providing system 1 according to the third embodiment changes the generation rule for gendering a new authentication symbol string, based on the number of times (frequency) at which an authentication symbol string has been updated. In the following, a structure for implementing such a function will be described.

[0160] FIG. 16 shows a functional block relevant to the present invention among those that are implemented in the content or application providing system 1 according to the third embodiment.

[0161] As shown in FIG. 16, the content or application providing system 1 according to the third embodiment differs from the first embodiment in that the former includes a first generation rule information storage unit 116, a first update frequency information storage unit 118, a second generation rule information storage unit 210, and a second update frequency information storage unit 212. For example, the first generation rule information storage unit 116 and the first update frequency information storage unit 118 are implemented using the auxiliary storage unit of the terminal device 10. The second generation rule information storage unit 210 and the second update frequency information storage unit 212 are implemented using the auxiliary storage unit of the server device 22 or the database 24.

[0162] The first update frequency information storage unit 118 stores update frequency information regarding the number of times at which the authentication symbol string stored in the first authentication symbol string storage unit 100 has been updated by the first authentication symbol string updating unit 114. FIG. 17 shows one example of the update frequency information stored in the first update frequency information storage unit 118.

[0163] The first generation rule information storage unit 116 stores generation rule information. Generation rule information is information for correlating the number of time (or frequency) at which an authentication symbol string has been updated and a generation rule for generating a new authentication symbol string based on an authentication symbol string. FIG. 18 shows one example of the generation rule information. In the generation rule information shown in FIG. 18, a generation rule for generating an authentication symbol string is correlated to a range of the number of times at which an authentication symbol string has been updated. In FIG. 18, "Ya" refers to a predetermined value. The "generation rule A" and the "generation rule B" are different rules from each other, being, for example, similar to those shown in FIGs 14 and 15.

[0164] The authentication symbol string generation unit 102 specifies a generation rule correlated to the frequency information stored in the first update frequency information storage unit 118, based on the generation rule information stored in the first generation rule information storage unit 116. Then, the authentication symbol string generation unit 102 uses that generation rule. That is, according to that generation rule, the authentication symbol string generation unit 102 generates a new authentication symbol string based on at least a part of the authentication symbol string stored in the first authentication symbol string storage unit 100.

[0165] For example, when generation rule information such as is shown in FIG. 18 is stored in the first generation rule information storage unit 116 and the update frequency (y) indicated by the update frequency information stored in the first update frequency information storage unit 118 satisfies "y<Ya", the authentication symbol string generation unit 102 uses the generation rule A. That is, according to the generation rule A, the authentication symbol string generation unit 102 generates a new authentication symbol string based on at least a part of the authentication symbol string stored in the first authentication symbol string storage unit 100.

[0166] The second update frequency information storage unit 212 stores so as to be correlated to a terminal ID, update frequency information regarding the number of times at which the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to that terminal ID has been updated by the second authentication symbol string updating unit 208. For example, in the third embodiment, a

terminal table such as is shown in FIG. 19 is stored. The terminal table shown in FIG. 19 differs from the terminal table shown in Fig. 6 in that the former includes an "update frequency information" field. In the "update frequency information" field, update frequency information regarding the number of times at which an authentication symbol string stored so as to be correlated to a terminal ID has been updated is stored.

[0167] Note that, on principle, in the second update frequency information storage unit 212 (terminal table), the update frequency information stored in the first update frequency information storage unit 118 of the terminal device 10 is stored so as to be correlated to the terminal ID of the terminal device 10. That is, for example, the update frequency information (twice) stored in the first update frequency information storage unit 118 of the terminal device 10 having the terminal ID "T00001" is stored in the second update frequency information storage unit 212 (terminal table) so as to be correlated to the terminal ID "T00001".

[0168] The second generation rule information storage unit 210 stores the generation rule information stored in the first generation rule information storage unit 116.

[0169] The determination unit 204 specifies a generation rule correlated to the update frequency information stored in the second update frequency information storage unit 212 so as to be correlated to the terminal ID received by the authentication information receiving unit 202, based on the generation rule information stored in the second generation rule information storage unit 210. Then, the determination unit 204 determines whether or not the authentication symbol string received by the authentication information receiving unit 202 belongs to the type of "an authentication symbol string that can be generated based on at least a part of the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202, according to the specified generation rule".

[0170] For example, when generation rule information such as is shown in Fig. 17 is stored in the second generation rule information storage unit 210 and the update frequency (y) indicated by the update frequency information stored in the second update frequency information storage unit 212 so as to be correlated to the terminal ID received by the authentication information receiving unit 202 satisfies "y<Ya", the determination unit 204 determines whether or not the authentication symbol string received by the authentication information receiving unit 202 belongs to the type of "an authentication symbol string that can be generated based on at least a part of the authentication symbol string stored in the second authentication symbol string storage unit 200 so as to be correlated to the terminal ID received by the authentication information receiving unit 202, according to the generation rule A".

[0171] Note that the functional blocks other than the first generation rule information storage unit 116, the second generation rule information storage unit 210, the authentication symbol string generation unit 102, and the determination unit 204 are similar to those in the first embodiment.

[0172] Below, processing executed in the content or application providing system 1 according to the third embodiment will be described. In the content or application providing system 1 according to the third embodiment as well, processing similar to that shown in FIGs 2, 4, 10, and 11 (or FIG. 12) is executed.

[0173] However, at step S207 in FIG. 4, the control unit of the terminal device 10 stores an authentication symbol string in the auxiliary storage unit (the first authentication symbol string storage unit 100) of the terminal device 10 and initializes the update frequency information stored in the auxiliary storage unit (the first update frequency information storage unit 118) of the terminal device 10 to the initial value (for example, 0) . Further, at step S208, the control unit of the server device 22 adds a new record to the terminal table, and registers the user ID, terminal ID, and authentication symbol string received at step S206 to the respective "user ID", "terminal ID", and "authentication symbol string" fields of the new record, and further, the initial value (for example, 0) in the "update frequency information" field.

[0174] Further, at step S301 in FIG. 10, the control unit of the terminal device 10 specifies a generation rule correlated to the update frequency information stored in the storage unit of the terminal device 10, based on the generation rule information, and uses the generation rule.

[0175] Further, at step S304 in FIG. 10, the control unit of the server device 22 accesses the terminal table to obtain the update frequency information stored so as to be correlated to the terminal ID received at step S302. Then, the control unit determines whether or not the authentication symbol string received at step S302 corresponds to "an authentication symbol string that can be generated based on at least a part of the authentication symbol string obtained at step S303, according to the generation rule correlated to the obtained update frequency information".

[0176] Further, at step S307 in FIG. 10, the control unit of the terminal device 10 updates the authentication symbol string stored in the auxiliary storage unit (the first authentication symbol string storage unit 100) of the terminal device 10, and increases by one the update frequency information stored in the auxiliary storage unit (the first update frequency information storage unit 118) of the terminal device 10. Similarly, at step S310, the control unit of the server device 22 updates the authentication symbol string stored in the terminal table (the second authentication symbol string storage unit 200) so as to be correlated to the terminal ID, and increases by one the update frequency information stored in the terminal table (the second update frequency information storage unit 212) so as to be correlated to the terminal ID.

[0177] Further, at step S405 in FIG. 11, the control unit

of the server device 22 obtains the authentication symbol string stored so as to be correlated to the terminal ID, and obtains the update frequency information stored so as to be correlated to the terminal ID. Then, at step S406, the control unit sends the update frequency information to the terminal device 10 together with the authentication symbol string. Further, at step S407, the control unit of the terminal device 10 updates the authentication symbol string stored in the auxiliary storage unit to the received authentication symbol string, and updates the update frequency information stored in the auxiliary storage unit to the received update frequency information.

[0178] Note that at step S405 in FIG. 11, the control unit of the server device 22 may obtain the authentication symbol string stored so as to be correlated to the terminal ID, and update the update frequency information stored so as to be correlated to the terminal ID to the initial value (for example, 0). Then, at step S407, the control unit of the terminal device 10 may update the authentication symbol string stored in the auxiliary storage unit to the received authentication symbol string, and updates the update frequency information stored in the auxiliary storage unit to the initial value (for example, 0).

[0179] Further, at step S507 in FIG. 12, the control unit of the terminal device 10 obtains the authentication symbol string stored in the auxiliary storage unit, and obtains also the update frequency information stored in the auxiliary storage unit. Then, at step S508, the control unit sends the update frequency information to the server device 22 together with the terminal ID and the authentication symbol string. Further, at step S509, the control unit of the server device 22 updates the authentication symbol string stored so as to be correlated to the terminal ID to the received authentication symbol string, and updates the update frequency information stored so as to be correlated to the terminal ID to the received update frequency information.

[0180] Note that at step S507 in FIG. 12, the control unit of the terminal device 10 may obtain the authentication symbol string stored in the auxiliary storage unit, and updates the update frequency information stored in the auxiliary storage unit to the initial value (for example, 0). Then, at step S509, the control unit of the server device 22 may update the authentication symbol string stored so as to be correlated to the terminal ID to the received authentication symbol string, and update the update frequency information stored so as to be correlated to the terminal ID to the initial value (for example, 0).

[0181] According to the content or application providing system 1 according to the third embodiment described above, similar to the content or application providing system 1 according to the second embodiment, it is possible to change the generation rule for generating a new authentication symbol string. According to the content or application providing system 1 according to the third embodiment, it is possible to enhance difficulty in prediction of an authentication symbol string. That is, according to the content or application providing system 1 according to the third embodiment, it is possible to make it more difficult for a person trying to illegally use content to predict an authentication symbol string.

[0182] Note that the present invention is not limited to the above-described first to third embodiments.

[1] For example, in the processing shown in FIG. 11, the authentication symbol string stored in the auxiliary storage unit of the terminal device 10 is updated to the authentication symbol string stored in the database 24 (the terminal table) so as to be correlated to the terminal ID of the terminal device 10 (see steps S405 to S407 in FIG. 11).

However, the authentication symbol string stored in the auxiliary storage unit of the terminal device 10 may be updated to a symbol string other than the authentication symbol string stored in the database 24 (the terminal table) so as to be correlated to the terminal ID of the terminal device 10.

At step S405 in FIG. 11, for example, instead of obtaining the authentication symbol string stored in the terminal table so as to be correlated to the terminal ID, an updating symbol string (in other words, an initializing symbol string) may be generated. For example, an updating symbol string may be generated at random. For example, the length of an updating symbol string may be determined at random, and the respective symbols constituting the updating symbol string as well may be determined at random. Then, at step S406, the generated updating symbol string is sent to the terminal device 10, and at step S407, the authentication symbol string stored in the auxiliary storage unit of the terminal device 10 may be updated to the updating symbol string.

Note that in the server device 22 in this case, after the processing at step S405 (and S406) executed, the authentication symbol string stored in the terminal table so as to be correlated to the terminal ID received at step S402 is updated to the generated updating symbol string.

In this manner as well, when a situation is resulted, due to deficiency or the like caused to the communication network 2, in which the authentication symbol string stored in the terminal device 10 does not coincide with that in the server device 22, an authentic user can initialize the situation so that the authentication symbol string stored in the terminal device 10 coincides with that in the server device 22. As a result, it is possible to ensure that an authentic user can use content.

[2] Further, for example, in the processing shown in FIG. 12, the authentication symbol string stored in the database 24 (the terminal table) so as to be correlated to the terminal ID of the terminal device 10 is updated to the authentication symbol string stored in the auxiliary storage unit of the terminal device 10 (see steps S507 to S509 in FIG. 12).

[0183] However, the authentication symbol string stored in the database 24 (terminal table) so as to be correlated to the terminal ID of the terminal device 10 may be updated to a symbol string other than the authentication symbol string stored in the auxiliary storage unit of the terminal device 10.

[0184] For example, at step S507 in FIG. 12, instead of obtaining the authentication symbol string stored in the terminal table so as to be correlated to the terminal ID, an updating symbol string (in other words, an initializing symbol string) may be generated. An updating symbol string may be generated at random. For example, the length of an updating symbol string may be determined at random, and the respective symbols constituting the updating symbol string may be determined at random. Then, at step S508, the generated updating symbol string is sent to the server device 22 together with the terminal ID, and at step S509, the authentication symbol string stored in the database 24 (terminal table) so as to be correlated to the terminal ID may be updated to the updating symbol string.

[0185] Note that in the terminal device 10 in this case, after the processing at step S507 (and S508) executed, the authentication symbol string stored in the auxiliary storage unit is updated to the generated updating symbol string.

[0186] In this manner as well, when a situation is resulted, due to deficiency or the like caused to the communication network 2, in which the authentication symbol string stored in the terminal device 10 does not coincide with that in the server device 22, an authentic user can initialize the situation so that the authentication symbol string stored in the terminal device 10 coincides with that in the server device 22. As a result, it is ensured that an authentic user can use content or an application.

Claims

1. A terminal device (10) for a user to use content or an application, connectable for communication to an authentication system (22), comprising:

authentication symbol string storage means (100) for storing an authentication symbol string;
authentication symbol string generation means (102) for generating a new authentication symbol string based on at least a part of the authentication symbol string stored in the authentication symbol string storage means (100), according to a generation rule for generating a new authentication symbol string based on an authentication symbol string;
authentication information transmission means (108) for sending terminal identification information for identifying the terminal device and the new authentication symbol string generated by the authentication symbol string generation means (102) to the authentication system (22);
means (110) for receiving notice information sent from the authentication system (22) in a case where it is determined in the authentication system (22) that the new authentication symbol string sent from the authentication information transmission means (108) belongs to a type of an authentication symbol string that is able to be generated, according to the generation rule, based on at least a part of an authentication symbol string stored in the authentication system (22) so as to be correlated to the terminal identification information sent by the authentication information transmission means (108);
permitting means (112) for permitting use of the content or the application, based on the notice information; and
authentication symbol string update means (114) for updating the authentication symbol string stored in the authentication symbol string storage means (100) to the new authentication symbol string generated by the authentication symbol string generation means (102) in the case where it is determined in the authentication system (22) that the new authentication symbol string sent from the authentication information transmission means (108) belongs to the type, wherein
in the case where it is determined in the authentication system (22) that the new authentication symbol string sent from the authentication information transmission means (108) belongs to the type, an authentication of the terminal device (10) is successful, and
the authentication symbol string stored in the authentication symbol string storage means (100) is updated each time the authentication of the terminal device is successful.

2. An authentication device (22) connectable for communication to a terminal device (10) for a user to use content or an application, comprising:

means for obtaining at least a part of content stored in authentication symbol string storage means (200) for storing an authentication symbol string so as to be correlated to terminal identification information for identifying the terminal device (10);
authentication information receiving means (202) for receiving from the terminal device (10), the terminal identification information and a new authentication symbol string generated based on at least a part of an authentication symbol string stored in the terminal device (10), according to a generation rule for generating a new authentication symbol string based on an authentication symbol string;

determination means (204) for determining whether or not the new authentication symbol string received by the authentication information receiving means (202) belongs to a type of an authentication symbol string that is able to be generated, according to the generation rule, based on at least a part of the authentication symbol string stored in the authentication symbol string storage means (200) so as to be correlated to the terminal identification information received by the authentication information receiving means (202) ;

notice information transmission means (206) for sending notice information for permitting use of the content or the application in the terminal device (10) to the terminal device (10) in a case where the determination means (204) determines that the new authentication symbol string received by the authentication information receiving means belongs to the type; and

authentication symbol string update means (208) for updating the authentication symbol string stored in the authentication symbol string storage means (200) so as to be correlated to the terminal identification information received by the authentication information receiving means (202) to the new authentication symbol string received by the authentication information receiving means (202), in the case where the determination means (204) determines that the new authentication symbol string received by the authentication information receiving means belongs to the type, wherein

in the case where the determination means (204) determines that the new authentication symbol string received by the authentication information receiving means (202) belongs to the type, an authentication of the terminal device (10) is successful, and

the authentication symbol string stored in the authentication symbol string storage means (200) is updated each time the authentication of the terminal device is successful.

3. A system (1) for providing content or an application including a terminal device (10) for a user to use the content or the application and an authentication system (22), wherein

the terminal device (10) being according to Claim 1;

the authentication system (22) being according to Claim 2.

4. The system (1) for providing the content or the application according to claim 3,

wherein

the terminal device (10) further includes first generation rule information storage means for storing generation rule information for correlating information on an authentication symbol string and a generation rule for generating a new authentication symbol string based on an authentication symbol string,

the authentication symbol string generation means (102) is arranged to specify a generation rule correlated to the authentication symbol string stored in the first authentication symbol string storage means (100), based on the generation rule information stored in the first generation rule information storage means, and generate the new authentication symbol string based on at least a part of the authentication symbol string stored in the first authentication symbol string storage means (100), according to the generation rule,

the authentication system (22) further includes second generation rule information storage means for storing the generation rule information stored in the first generation rule information storage means, and the determination means (204) is arranged to specify a generation rule correlated to the authentication symbol string stored in the second authentication symbol string storage means (200), based on the generation rule information stored in the second generation rule information storage means, and determine whether or not the new authentication symbol string received by the authentication information receiving means (202) belongs to a type of an authentication symbol string that is able to be generated, according to the generation rule, based on at least a part of the authentication symbol string stored in the second authentication symbol string storage means (200) so as to be correlated to the terminal identification information received by the authentication information receiving means (202) .

5. The system (1) for providing the content or the application according to claim 4,

wherein

the generation rule information is information for correlating a length of an authentication symbol string and a generation rule for generating a new authentication symbol string based on an authentication symbol string,

the authentication symbol string generation means (102) is arranged to generate the new authentication symbol string based on at least a part of the authentication symbol string stored in the first authentication symbol string storage means (100), according to a generation rule correlated to a length of the authentication symbol string stored in the first authentication symbol string storage means (100) and

the determination means (204) is arranged to determine whether or not the new authentication symbol string received by the authentication information receiving means belongs to a type of an authentication symbol string that is able to be generated, according to a generation rule correlated to a length of the authentication symbol string stored in the second au-

thentication symbol string storage means (200), based on at least a part of the authentication symbol string stored in the second authentication symbol string storage means (200) so as to be correlated to the terminal identification information received by the authentication information receiving means (202).

6. The system (1) for providing the content or the application according to claim 4,
wherein
the generation rule information is information for correlating a type of a symbol at a predetermined position in an authentication symbol string and a generation rule for generating a new authentication symbol string based on an authentication symbol string,
the authentication symbol string generation means (102) is arranged to generate the new authentication symbol string based on at least a part of the authentication symbol string stored in the first authentication symbol string storage means (100), according to a generation rule correlated to a type of a symbol at the predetermined position in the authentication symbol string stored in the first authentication symbol string storage means (100), and
the determination means (204) is arranged to determine whether or not the new authentication symbol string received by the authentication information receiving means (202) belongs to a type of an authentication symbol string that is able to be generated, according to a generation rule correlated to a type of a symbol at the predetermined position in the authentication symbol string stored in the second authentication symbol string storage means (200), based on at least a part of the authentication symbol string stored in the second authentication symbol string storage means (200) so as to be correlated to the terminal identification information received by the authentication information receiving means (202).

7. The system (1) for providing the content or the application according to any of claims 3 to 6 wherein
the terminal device (10) further includes

means for guiding the user to input user identification information for identifying the user and a user password, and
means for sending the user identification information and the user password input by the user to the authentication system (22),

the authentication system (22) further includes

user authentication information storage means for storing a combination of the user identification information and the user password, and
means for determining whether or not the combination of the user identification information and the user password sent from the terminal device is any of combinations of user identification information and a user password stored in the user authentication information storage means, and

the authentication system (22) is arranged to set the authentication symbol string stored in the first authentication symbol string storage means (100) and the authentication symbol string stored in the second authentication symbol string storage means (200) so as to be correlated to terminal identification information correlated to the user identification information sent from the terminal device (10), to a same authentication symbol string, in a case where it is determined that the combination of the user identification information and the user password sent from the terminal device is any of the combinations of the user identification information and the user password stored in the user authentication information storage means.

8. The system (1) for providing the content or the application according to claim 3,
wherein
the terminal device (10) further includes

first update frequency information storage means (118) for storing update frequency information concerning a number of times at which the authentication symbol string stored in the first authentication symbol string storage means (100) is updated, and
first generation rule information storage means (116) for storing generation rule information for correlating a number of times at which an authentication symbol string is updated and a generation rule for generating a new authentication symbol string based on an authentication symbol string,

the authentication symbol string generation means (102) is arranged to specify a generation rule correlated to the update frequency information stored in the first update frequency information storage means, based on the generation rule information stored in the first generation rule information storage means, and generate the new authentication symbol string based on at least a part of the authentication symbol string stored in the first authentication symbol string storage means (100), according to the generation rule,
the authentication system (22) further includes

second update frequency information storage means (212) for storing update frequency information so as to be correlated to the terminal identification information, the update frequency information concerning a number of times at

which the authentication symbol string stored in the second authentication symbol string storage means so as to be correlated to the terminal identification information is updated, and
second generation rule information storage means (210) for storing the generation rule information stored in the first generation rule information storage means, and

the determination means (204) is arranged to specify a generation rule correlated to the update frequency information stored in the second update frequency information storage means (212) so as to be correlated to the terminal identification information received by the authentication information receiving means (202), based on the generation rule information stored in the second generation rule information storage means (210), and determine whether or not the new authentication symbol string received by the authentication information receiving means (202) belongs to a type of an authentication symbol string that is able to be generated, according to the generation rule, based on at least a part of the authentication symbol string stored in the second authentication symbol string storage means (200) so as to be correlated to the terminal identification information received by the authentication information receiving means (202).

9. The system (1) for providing the content or the application according to claim 8, wherein
the terminal device (10) includes

means for guiding the user to input user identification information for identifying the user and a user password, and
means for sending the user identification information and the user password input by the user to the authentication system,

the authentication system further includes

user authentication information storage means for storing a combination of the user identification information and the user password, and
means for determining whether or not the combination of the user identification information and the user password sent from the terminal device is any of combinations of user identification information and a user password stored in the user authentication information storage means, and

the authentication system (22) is arranged to set the authentication symbol string stored in the first authentication symbol string storage means (100) and the authentication symbol string stored in the second authentication symbol string storage means (200) so as to be correlated to terminal identification information correlated to the user identification information sent from the terminal device (10), to a same authentication symbol string, and set the update frequency information stored in the first update frequency information storage means (118) and the update frequency information stored in the second update frequency information storage means (212) so as to be correlated to the terminal identification information correlated to the user identification information sent from the terminal device (10), to a same update frequency, in a case where it is determined that the combination of the user identification information and the user password sent from the terminal device (10) is any of the combinations of the user identification information and the user password stored in the user authentication information storage means.

10. The system (1) for providing the content or the application according to any of claims 3 to 9, wherein
the generation rule includes a rule in which a symbol at which position in an authentication symbol string is to be extracted, and
the authentication symbol string generation means (102) includes extraction means (104) for extracting, according to the generation rule, one or more symbols from the authentication symbol string stored in the first authentication symbol string storage means, and generate the new authentication symbol string based on the one or more symbols extracted by the extraction means (104).

11. The system (1) for providing the content or the application according to any of claims 3 to 10, wherein
the generation rule includes at least one of a rule for converting one symbol in an authentication symbol string into one symbol, a rule for converting one symbol in an authentication symbol string into a plurality of symbols, a rule for converting a plurality of symbols in an authentication symbol string to one symbol, and a rule for converting a plurality of symbols in an authentication symbol string into a plurality of symbols, and
the authentication symbol string generation means (102) includes conversion means (106) for converting at least a part of the authentication symbol string stored in the first authentication symbol string storage means (100) according to the generation rule to obtain one or more symbols, and generate the new authentication symbol string based on the one or more symbols obtained by the conversion means (106).

12. The system (1) for providing the content or the application according to any of claims 3 to 11, wherein
the generation rule includes a rule in which one or more symbols based on at least a part of an authentication symbol string is/are to be included in which

position in the new authentication symbol string, and the authentication symbol string generation means (102) is arranged to generate, according to the generation rule, a symbol string including one or more symbols based on at least a part of the authentication symbol string stored in the first authentication symbol string storage means (100) as the new authentication symbol string.

13. A control method for a terminal device for a user to use content or an application, connected for communication to an authentication system, the control method comprising:

a step of obtaining an authentication symbol string stored in authentication symbol string storage means for storing the authentication symbol string;
an authentication symbol string generation step (S301) of generating a new authentication symbol string based on at least a part of the authentication symbol string stored in the authentication symbol string storage means, according to a generation rule for generating a new authentication symbol string based on an authentication symbol string;
an authentication information transmission step (S302) of sending terminal identification information for identifying the terminal device and the new authentication symbol string generated at the authentication symbol string generation step to the authentication system;
a step of receiving notice information (S305) sent from the authentication system in a case where it is determined in the authentication system that the new authentication symbol string sent at the authentication information transmission step belongs to a type of an authentication symbol string that is able to be generated, according to the generation rule, based on at least a part of an authentication symbol string stored in the authentication system so as to be correlated to the terminal identification information sent at the authentication information transmission step;
a permitting step (S308) of permitting use of the content or the application, based on the notice information; and
an authentication symbol string update step (S307) of updating the authentication symbol string stored in the authentication symbol string storage means to the new authentication symbol string generated at the authentication symbol string generation step in the case where it is determined in the authentication system that the new authentication symbol string sent at the authentication information transmission step belongs to the type, wherein
in the case where it is determined in the authentication system that the new authentication symbol string sent by the authentication information transmission step (S302) belongs to the type, an authentication of the terminal device is successful, and the control method further comprising the step of:
updating the authentication symbol string stored in the authentication symbol string storage means each time the authentication of the terminal device is successful.

14. A control method for an authentication device connected for communication to a terminal device for a user to use content or an application, the control method comprising:

a step (S303) of obtaining, at least a part of content stored in authentication symbol string storage means for storing an authentication symbol string so as to be correlated to terminal identification information for identifying the terminal device;
an authentication information receiving step (S302) of receiving from the terminal device, the terminal identification information and a new authentication symbol string generated based on at least a part of an authentication symbol string stored in the terminal device, according to a generation rule for generating a new authentication symbol string, based on an authentication symbol string;
a determination step (S304) of determining whether or not the new authentication symbol string received at the authentication information receiving step belongs to a type of an authentication symbol string that is able to be generated, according to the generation rule, based on at least a part of the authentication symbol string stored in the authentication symbol string storage means so as to be correlated to the terminal identification information received at the authentication information receiving step;
a notice information transmission step (S305) of sending notice information for permitting use of the content or the application in the terminal device to the terminal device in a case where it is determined at the determination step that the new authentication symbol string received at the authentication information receiving step belongs to the type; and
an authentication symbol string update step (S310) of updating the authentication symbol string stored in the authentication symbol string storage means so as to be correlated to the terminal identification information received at the authentication information receiving step to the new authentication symbol string received at the

authentication information receiving step, in the case where it is determined at the determination step that the new authentication symbol string received at the authentication information receiving step belongs to the type, wherein
in the case where the determination step (S304) determines that the new authentication symbol string received by the authentication information receiving step (S302) belongs to the type, an authentication of the terminal device is successful, and the control method further comprising the step of:
updating the authentication symbol string stored in the authentication symbol string storage means each time the authentication of the terminal device is successful.

15. A control method for a system for providing content or an application including a terminal device for a user to use the content or the application and an authentication system, comprising:

a control method for the terminal device being according to Claim 13; and
a control method for the authentication system being according to Claim 14.

16. A program for causing a computer to function as a terminal device for a user to use content or an application, connected for communication to an authentication system, the program for causing the computer to function as the terminal device according to Claim 1.

17. A program for causing a computer to function as an authentication device connected for communication to a terminal device for a user to use content or an application, the program for causing the computer to function as the authentication device according to Claim 2.

18. A computer readable information storage medium storing the program according to claim 16 or 17.

Patentansprüche

1. Endgerätvorrichtung (10) für einen Benutzer, um Inhalt oder eine Anwendung zu verwenden, die zur Kommunikation mit einem Authentifizierungssystem (22) verbindbar ist, umfassend:

Authentifizierungssymbolfolge-Speichermittel (100) zum Speichern einer Authentifizierungssymbolfolge;
Authentifizierungssymbolfolge-Erzeugungsmittel (102) zum Erzeugen einer neuen Authentifizierungssymbolfolge auf Basis mindestens eines Teils der Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel (100) gespeichert ist, gemäß einer Erzeugungsregel zum Erzeugen einer neuen Authentifizierungssymbolfolge auf Basis einer Authentifizierungssymbolfolge;
Authentifizierungsinformation-Übertragungsmittel (108) zum Senden von Endgerät-Identifikationsinformation zum Identifizieren der Endgerätvorrichtung , und der vom Authentifizierungssymbolfolge-Erzeugungsmittel (102) erzeugten neuen Authentifizierungssymbolfolge an das Authentifizierungssystem (22);
Mittel (110) zum Empfangen von Hinweisinformation, die vom Authentifizierungssystem (22) gesendet wird in einem Fall, in dem im Authentifizierungssystem (22) bestimmt wird, dass die vom Authentifizierungsinformation-Übertragungsmittel (108) gesendete neue Authentifizierungssymbolfolge zu einem Typ einer Authentifizierungssymbolfolge gehört, die imstande ist, gemäß der Erzeugungsregel auf Basis mindestens eines Teils einer Authentifizierungssymbolfolge, die im Authentifizierungssystem (22) gespeichert ist, so erzeugt zu werden, dass sie mit der vom Authentifizierungsinformation-Übertragungsmittel (108) gesendeten Endgerät-Identifikationsinformation korreliert ist;
Ermöglichungsmittel (112) zum Ermöglichen einer Verwendung des Inhalts oder der Anwendung auf Basis der Hinweisinformation; und
Authentifizierungssymbolfolge-Aktualisierungsmittel (114) zum Aktualisieren der Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel (100) gespeichert ist, auf die vom Authentifizierungssymbolfolge-Erzeugungsmittel (102) erzeugte neue Authentifizierungssymbolfolge in dem Fall, in dem im Authentifizierungssystem (22) bestimmt wird, dass die vom Authentifizierungsinformation-Übertragungsmittel (108) gesendete neue Authentifizierungssymbolfolge zu dem Typ gehört, wobei
in dem Fall, in dem im Authentifizierungssystem (22) bestimmt wird, dass die vom Authentifizierungsinformation-Übertragungsmittel (108) gesendete neue Authentifizierungssymbolfolge zu dem Typ gehört, eine Authentifizierung der Endgerätvorrichtung (10) erfolgreich ist, und
die Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel (100) gespeichert ist, jedes Mal aktualisiert wird, wenn die Authentifizierung der Endgerätvorrichtung erfolgreich ist.

2. Authentifizierungsvorrichtung (22), die zur Kommunikation mit einer Endgerätvorrichtung (10) für einen

Benutzer verbindbar ist, um Inhalt oder eine Anwendung zu verwenden, umfassend:

Mittel zum Erhalten von mindestens einem Teil von Inhalt, der im Authentifizierungssymbolfolge-Speichermittel (200) zum Speichern einer Authentifizierungssymbolfolge so gespeichert ist, dass er mit Endgerät-Identifikationsinformation zum Identifizieren der Endgerätvorrichtung (10) korreliert ist;

Authentifizierungsinformation-Empfangsmittel (202) zum Empfangen, von der Endgerätvorrichtung (10), der Endgerät-Identifikationsinformation und einer neuen Authentifizierungssymbolfolge, die auf Basis mindestens eines Teils einer Authentifizierungssymbolfolge, die in der Endgerätvorrichtung (10) gespeichert ist, gemäß einer Erzeugungsregel zum Erzeugen einer neuen Authentifizierungssymbolfolge auf Basis einer Authentifizierungssymbolfolge erzeugt wurde;

Bestimmungsmittel (204) zum Bestimmen, ob die vom Authentifizierungsinformation-Empfangsmittel (202) empfangene neue Authentifizierungssymbolfolge zu einem Typ einer Authentifizierungssymbolfolge gehört oder nicht, die imstande ist, gemäß der Erzeugungsregel auf Basis mindestens eines Teils der Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel (200) gespeichert ist, so erzeugt zu werden, dass sie mit der vom Authentifizierungsinformation-Empfangsmittel (202) empfangenen Endgerät-Identifikationsinformation korreliert ist;

Hinweisinformation-Übertragungsmittel (206) zum Senden von Hinweisinformation zum Ermöglichen einer Verwendung des Inhalts oder der Anwendung in der Endgerätvorrichtung (10) an die Endgerätvorrichtung (10) in einem Fall, in dem das Bestimmungsmittel (204) bestimmt, dass die vom Authentifizierungsinformation-Empfangsmittel empfangene neue Authentifizierungssymbolfolge zu dem Typ gehört; und

Authentifizierungssymbolfolge-Aktualisierungsmittel (208) zum Aktualisieren der Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel (200) so gespeichert ist, dass sie mit der vom Authentifizierungsinformation-Empfangsmittel (202) empfangenen Endgerät-Identifikationsinformation korreliert ist, auf die vom Authentifizierungsinformation-Empfangsmittel (202) empfangene neue Authentifizierungssymbolfolge in dem Fall, in dem das Bestimmungsmittel (204) bestimmt, dass die vom Authentifizierungsinformation-Empfangsmittel empfangene neue Authentifizierungssymbolfolge zu dem Typ gehört, wobei

in dem Fall, in dem das Bestimmungsmittel (204) bestimmt, dass die vom Authentifizierungsinformation-Empfangsmittel (202) empfangene neue Authentifizierungssymbolfolge zu dem Typ gehört, eine Authentifizierung der Endgerätvorrichtung (10) erfolgreich ist, und

die Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel (200) gespeichert ist, jedes Mal aktualisiert wird, wenn die Authentifizierung der Endgerätvorrichtung erfolgreich ist.

3. System (1) zum Bereitstellen von Inhalt oder einer Anwendung, das eine Endgerätvorrichtung (10) für einen Benutzer, um den Inhalt oder die Anwendung zu verwenden, und ein Authentifizierungssystem (22) einschließt, wobei

die Endgerätvorrichtung (10) nach Anspruch 1 ist;

das Authentifizierungssystem (22) nach Anspruch 2 ist.

4. System (1) zum Bereitstellen des Inhalts oder der Anwendung nach Anspruch 3,

wobei

die Endgerätvorrichtung (10) weiter erste Erzeugungsregelinformation-Speichermittel zum Speichern von Erzeugungsregelinformation zum Korrelieren von Information bezüglich einer Authentifizierungssymbolfolge und einer Erzeugungsregel zum Erzeugen einer neuen Authentifizierungssymbolfolge auf Basis einer Authentifizierungssymbolfolge einschließt,

das Authentifizierungssymbolfolge-Erzeugungsmittel (102) dazu eingerichtet ist, auf Basis der Erzeugungsregelinformation, die im ersten Erzeugungsregelinformation-Speichermittel gespeichert ist, eine Erzeugungsregel zu spezifizieren, die mit der im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeicherten Authentifizierungssymbolfolge korreliert ist, und die neue Authentifizierungssymbolfolge gemäß der Erzeugungsregel auf Basis mindestens eines Teils der im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeicherten Authentifizierungssymbolfolge zu erzeugen,

das Authentifizierungssystem (22) weiter zweite Erzeugungsregelinformation-Speichermittel zum Speichern der im ersten Erzeugungsregelinformation-Speichermittel gespeicherten Erzeugungsregelinformation einschließt, und

das Bestimmungsmittel (204) dazu eingerichtet ist, auf Basis der Erzeugungsregelinformation, die im zweiten Erzeugungsregelinformation-Speichermittel gespeichert ist, eine Erzeugungsregel zu spezifizieren, die mit der im zweiten Authentifizierungssymbolfolge-Speichermittel (200) gespeicherten Authentifizierungssymbolfolge korreliert ist, und zu bestimmen, ob die vom Authentifizierungsinformation-Empfangsmittel (202) empfangene neue Authen-

tifizierungssymbolfolge zu einem Typ einer Authentifizierungssymbolfolge gehört oder nicht, die imstande ist, gemäß der Erzeugungsregel auf Basis mindestens eines Teils der Authentifizierungssymbolfolge, die im zweiten Authentifizierungssymbolfolge-Speichermittel (200) gespeichert ist, so erzeugt zu werden, dass sie mit der vom Authentifizierungsinformation-Empfangsmittel (202) empfangenen Endgerät-Identifikationsinformation korreliert ist.

5. System (1) zum Bereitstellen des Inhalts oder der Anwendung nach Anspruch 4,
wobei
die Erzeugungsregelinformation Information zum Korrelieren einer Länge einer Authentifizierungssymbolfolge und einer Erzeugungsregel zum Erzeugen einer neuen Authentifizierungssymbolfolge auf Basis einer Authentifizierungssymbolfolge ist,
das Authentifizierungssymbolfolge-Erzeugungsmittel (102) dazu eingerichtet ist, die neue Authentifizierungssymbolfolge gemäß einer Erzeugungsregel, die mit einer Länge der im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeicherten Authentifizierungssymbolfolge korreliert ist, auf Basis mindestens eines Teils der im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeicherten Authentifizierungssymbolfolge zu erzeugen, und
das Bestimmungsmittel (204) dazu eingerichtet ist, zu bestimmen, ob die vom Authentifizierungsinformation-Empfangsmittel empfangene neue Authentifizierungssymbolfolge zu einem Typ einer Authentifizierungssymbolfolge gehört oder nicht, die imstande ist, gemäß einer Erzeugungsregel, die mit einer Länge der im zweiten Authentifizierungssymbolfolge-Speichermittel (200) gespeicherten Authentifizierungssymbolfolge korreliert ist, auf Basis mindestens eines Teils der im zweiten Authentifizierungssymbolfolge-Speichermittel (200) gespeicherten Authentifizierungssymbolfolge so erzeugt zu werden, dass sie mit der vom Authentifizierungsinformation-Empfangsmittel (202) empfangenen Endgerät-Identifikationsinformation korreliert ist.

6. System (1) zum Bereitstellen des Inhalts oder der Anwendung nach Anspruch 4,
wobei
die Erzeugungsregelinformation Information zum Korrelieren eines Typs eines Symbols an einer vorbestimmten Stelle in einer Authentifizierungssymbolfolge und einer Erzeugungsregel zum Erzeugen einer neuen Authentifizierungssymbolfolge auf Basis einer Authentifizierungssymbolfolge ist,
das Authentifizierungssymbolfolge-Erzeugungsmittel (102) dazu eingerichtet ist, die neue Authentifizierungssymbolfolge gemäß einer Erzeugungsregel, die mit einem Typ eines Symbols an der vorbestimmten Stelle in der im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeicherten Authentifizierungssymbolfolge korreliert ist, auf Basis mindestens eines Teils der im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeicherten Authentifizierungssymbolfolge zu erzeugen, und
das Bestimmungsmittel (204) dazu eingerichtet ist, zu bestimmen, ob die vom Authentifizierungsinformation-Empfangsmittel (202) empfangene neue Authentifizierungssymbolfolge zu einem Typ einer Authentifizierungssymbolfolge gehört oder nicht, die imstande ist, gemäß einer Erzeugungsregel, die mit einem Typ eines Symbols an der vorbestimmten Stelle in der im zweiten Authentifizierungssymbolfolge-Speichermittel (200) gespeicherten Authentifizierungssymbolfolge korreliert ist, auf Basis mindestens eines Teils der im zweiten Authentifizierungssymbolfolge-Speichermittel (200) gespeicherten Authentifizierungssymbolfolge so erzeugt zu werden, dass sie mit der vom Authentifizierungsinformation-Empfangsmittel (202) empfangenen Endgerät-Identifikationsinformation korreliert ist.

7. System (1) zum Bereitstellen des Inhalts oder der Anwendung nach einem der Ansprüche 3 bis 6, wobei
die Endgerätvorrichtung (10) weiter einschließt

Mittel zum Anleiten des Benutzers dazu, Benutzeridentifikationsinformation zum Identifizieren des Benutzers, und ein Benutzerkennwort einzugeben, und
Mittel zum Senden der Benutzeridentifikationsinformation und des Benutzerkennworts, die vom Benutzer eingegeben wurden, an das Authentifizierungssystem (22),

das Authentifizierungssystem (22) weiter einschließt

Benutzerauthentifizierungsinformation-Speichermittel zum Speichern einer Kombination der Benutzeridentifikationsinformation und des Benutzerkennworts, und
Mittel zum Bestimmen, ob die Kombination der Benutzeridentifikationsinformation und des Benutzerkennworts, die von der Endgerätvorrichtung gesendet wird, eine beliebige von Kombinationen von Benutzeridentifikationsinformation und einem Benutzerkennwort ist oder nicht, die im Benutzerauthentifizierungsinformation-Speichermittel gespeichert sind, und

das Authentifizierungssystem (22) dazu eingerichtet ist, die Authentifizierungssymbolfolge, die im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeichert ist, und die Authentifizierungssymbolfolge, die im zweiten Authentifizierungssymbolfolge-

Speichermittel (200) so gespeichert ist, dass sie mit Endgerät-Identifikationsinformation korreliert ist, die mit der von der Endgerätvorrichtung (10) gesendeten Benutzeridentifikationsinformation korreliert ist, auf eine gleiche Authentifizierungssymbolfolge einzustellen in einem Fall, in dem bestimmt wird, dass die Kombination der Benutzeridentifikationsinformation und des Benutzerkennworts, die von der Endgerätvorrichtung gesendet wird, eine beliebige von den Kombinationen der Benutzeridentifikationsinformation und des Benutzerkennworts ist, die im Benutzerauthentifizierungsinformation-Speichermittel gespeichert sind.

8. System (1) zum Bereitstellen des Inhalts oder der Anwendung nach Anspruch 3,
wobei
die Endgerätvorrichtung (10) weiter einschließt

erste Aktualisierungsfrequenzinformation-Speichermittel (118) zum Speichern von Aktualisierungsfrequenzinformation betreffend einer Anzahl von Malen, bei denen die Authentifizierungssymbolfolge, die im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeichert ist, aktualisiert wird, und
erste Erzeugungsregelinformation-Speichermittel (116) zum Speichern von Erzeugungsregelinformation zum Korrelieren einer Anzahl von Malen, bei denen eine Authentifizierungssymbolfolge aktualisiert wird, und einer Erzeugungsregel zum Erzeugen einer neuen Authentifizierungssymbolfolge auf Basis einer Authentifizierungssymbolfolge,

das Authentifizierungssymbolfolge-Erzeugungsmittel (102) dazu eingerichtet ist, auf Basis der im ersten Erzeugungsregelinformation-Speichermittel gespeicherten Erzeugungsregelinformation eine Erzeugungsregel zu spezifizieren, die mit der im ersten Aktualisierungsfrequenzinformation-Speichermittel gespeicherten Aktualisierungsfrequenzinformation korreliert ist, und die neue Authentifizierungssymbolfolge gemäß der Erzeugungsregel auf Basis mindestens eines Teils der im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeicherten Authentifizierungssymbolfolge zu erzeugen,
das Authentifizierungssystem (22) weiter einschließt

zweite Aktualisierungsfrequenzinformation-Speichermittel (212) zum Speichern von Aktualisierungsfrequenzinformation so, dass sie mit der Endgerät-Identifikationsinformation korreliert ist, wobei die Aktualisierungsfrequenzinformation eine Anzahl von Malen betrifft, bei denen die Authentifizierungssymbolfolge, die im zweiten Authentifizierungssymbolfolge-Speichermittel so gespeichert ist, dass sie mit der Endgerät-Identifikationsinformation korreliert ist, aktualisiert wird, und
zweite Erzeugungsregelinformation-Speichermittel (210) zum Speichern der im ersten Erzeugungsregelinformation-Speichermittel gespeicherten Erzeugungsregelinformation, und

das Bestimmungsmittel (204) dazu eingerichtet ist, auf Basis der im zweiten Erzeugungsregelinformation-Speichermittel (210) gespeicherten Erzeugungsregelinformation eine Erzeugungsregel zu spezifizieren, die mit der Aktualisierungsfrequenzinformation korreliert ist, die im zweiten Aktualisierungsfrequenzinformation-Speichermittel (212) so gespeichert ist, dass sie mit der vom Authentifizierungsinformation-Empfangsmittel (202) empfangenen Endgerät-Identifikationsinformation korreliert ist, und zu bestimmen, ob die vom Authentifizierungsinformation-Empfangsmittel (202) empfangene neue Authentifizierungssymbolfolge zu einem Typ einer Authentifizierungssymbolfolge gehört oder nicht, die imstande ist, gemäß der Erzeugungsregel auf Basis mindestens eines Teils der im zweiten Authentifizierungssymbolfolge-Speichermittel (200) gespeicherten Authentifizierungssymbolfolge so erzeugt zu werden, dass sie mit der vom Authentifizierungsinformation-Empfangsmittel (202) empfangenen Endgerät-Identifikationsinformation korreliert ist.

9. System (1) zum Bereitstellen des Inhalts oder der Anwendung nach Anspruch 8, wobei
die Endgerätvorrichtung (10) einschließt

Mittel zum Anleiten des Benutzers dazu, Benutzeridentifikationsinformation zum Identifizieren des Benutzers, und ein Benutzerkennwort einzugeben, und
Mittel zum Senden der Benutzeridentifikationsinformation und des Benutzerkennworts, die vom Benutzer eingegeben wurden, an das Authentifizierungssystem,

das Authentifizierungssystem weiter einschließt

Benutzerauthentifizierungsinformation-Speichermittel zum Speichern einer Kombination der Benutzeridentifikationsinformation und des Benutzerkennworts, und
Mittel zum Bestimmen, ob die Kombination der Benutzeridentifikationsinformation und des Benutzerkennworts, die von der Endgerätvorrichtung gesendet wird, eine beliebige von Kombinationen von Benutzeridentifikationsinformation und einem Benutzerkennwort ist oder nicht, die im Benutzerauthentifizierungsinformation-Speichermittel gespeichert sind, und

das Authentifizierungssystem (22) dazu eingerichtet ist, die Authentifizierungssymbolfolge, die im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeichert ist, und die Authentifizierungssymbolfolge, die im zweiten Authentifizierungssymbolfolge-Speichermittel (200) so gespeichert ist, dass sie mit Endgerät-Identifikationsinformation korreliert ist, die mit der von der Endgerätvorrichtung (10) gesendeten Benutzeridentifikationsinformation korreliert ist, auf eine gleiche Authentifizierungssymbolfolge einzustellen, und die Aktualisierungsfrequenzinformation, die im ersten Aktualisierungsfrequenzinformation-Speichermittel (118) gespeichert ist, und die Aktualisierungsfrequenzinformation, die im zweiten Aktualisierungsfrequenzinformation-Speichermittel (212) so gespeichert ist, dass sie mit der Endgerät-Identifikationsinformation korreliert ist, die mit der von der Endgerätvorrichtung (10) gesendeten Benutzeridentifikationsinformation korreliert ist, auf eine gleiche Aktualisierungsfrequenz einzustellen in einem Fall, in dem bestimmt wird, dass die Kombination der Benutzeridentifikationsinformation und des Benutzerkennworts, die von der Endgerätvorrichtung (10) gesendet wird, eine beliebige von den Kombinationen der Benutzeridentifikationsinformation und des Benutzerkennworts ist, die im Benutzerauthentifizierungsinformation-Speichermittel gespeichert sind.

10. System (1) zum Bereitstellen des Inhalts oder der Anwendung nach einem der Ansprüche 3 bis 9, wobei
die Erzeugungsregel eine Regel einschließt, nach der ein Symbol an welcher Stelle in einer Authentifizierungssymbolfolge extrahiert werden soll, und
das Authentifizierungssymbolfolge-Erzeugungsmittel (102) Extraktionsmittel (104) einschließt zum Extrahieren, gemäß der Erzeugungsregel, von einem oder mehreren Symbolen aus der im ersten Authentifizierungssymbolfolge-Speichermittel gespeicherten Authentifizierungssymbolfolge, und Erzeugen der neuen Authentifizierungssymbolfolge auf Basis des einen oder der mehreren vom Extraktionsmittel (104) extrahierten Symbole.

11. System (1) zum Bereitstellen des Inhalts oder der Anwendung nach einem der Ansprüche 3 bis 10, wobei
die Erzeugungsregel mindestens eines einschließt aus einer Regel zum Konvertieren eines Symbols in einer Authentifizierungssymbolfolge in ein Symbol, einer Regel zum Konvertieren eines Symbols in einer Authentifizierungssymbolfolge in eine Vielzahl von Symbolen, einer Regel zum Konvertieren einer Vielzahl von Symbolen in einer Authentifizierungssymbolfolge in ein Symbol, und einer Regel zum Konvertieren einer Vielzahl von Symbolen in einer Authentifizierungssymbolfolge in eine Vielzahl von Symbolen, und
das Authentifizierungssymbolfolge-Erzeugungsmittel (102) Konvertierungsmittel (106) einschließt zum Konvertieren mindestens eines Teils der im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeicherten Authentifizierungssymbolfolge gemäß der Erzeugungsregel, um ein oder mehrere Symbole zu erhalten, und die neue Authentifizierungssymbolfolge auf Basis des einen oder der mehreren vom Konvertierungsmittel (106) erhaltenen Symbole zu erzeugen.

12. System (1) zum Bereitstellen des Inhalts oder der Anwendung nach einem der Ansprüche 3 bis 11, wobei
die Erzeugungsregel eine Regel einschließt, nach der ein oder mehrere Symbole auf Basis mindestens eines Teils einer Authentifizierungssymbolfolge an welcher Stelle in der neuen Authentifizierungssymbolfolge eingeschlossen werden soll/sollen, und
das Authentifizierungssymbolfolge-Erzeugungsmittel (102) dazu eingerichtet ist, gemäß der Erzeugungsregel eine Symbolfolge, die ein oder mehrere Symbole einschließt, auf Basis mindestens eines Teils der im ersten Authentifizierungssymbolfolge-Speichermittel (100) gespeicherten Authentifizierungssymbolfolge als die neue Authentifizierungssymbolfolge zu erzeugen.

13. Steuerungsverfahren für eine Endgerätvorrichtung für einen Benutzer, um Inhalt oder eine Anwendung zu verwenden, die zur Kommunikation mit einem Authentifizierungssystem verbunden ist, wobei das Steuerungsverfahren umfasst:

einen Schritt des Erhaltens einer Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel zum Speichern der Authentifizierungssymbolfolge gespeichert ist;
einen Authentifizierungssymbolfolge-Erzeugungsschritt (S301) des Erzeugens einer neuen Authentifizierungssymbolfolge auf Basis mindestens eines Teils der Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel gespeichert ist, gemäß einer Erzeugungsregel zum Erzeugen einer neuen Authentifizierungssymbolfolge auf Basis einer Authentifizierungssymbolfolge;
einen Authentifizierungsinformation-Übertragungsschritt (S302) des Sendens von Endgerät-Identifikationsinformation zum Identifizieren der Endgerätvorrichtung, und der beim Authentifizierungssymbolfolge-Erzeugungsschritt erzeugten neuen Authentifizierungssymbolfolge an das Authentifizierungssystem;
einen Schritt des Empfangens von Hinweisinformation (S305), die vom Authentifizierungssystem gesendet wird in einem Fall, in dem im

Authentifizierungssystem bestimmt wird, dass die beim Authentifizierungsinformation-Übertragungsschritt gesendete neue Authentifizierungssymbolfolge zu einem Typ einer Authentifizierungssymbolfolge gehört, die imstande ist, gemäß der Erzeugungsregel auf Basis mindestens eines Teils einer Authentifizierungssymbolfolge, die im Authentifizierungssystem gespeichert ist, so erzeugt zu werden, dass sie mit der beim Authentifizierungsinformation-Übertragungsschritt gesendeten Endgerät-Identifikationsinformation korreliert ist;

einen Ermöglichungsschritt (S308) des Ermöglichens einer Verwendung des Inhalts oder der Anwendung auf Basis der Hinweisinformation; und

einen Authentifizierungssymbolfolge-Aktualisierungsschritt (S307) des Aktualisierens der im Authentifizierungssymbolfolge-Speichermittel gespeicherten Authentifizierungssymbolfolge auf die beim Authentifizierungssymbolfolge-Erzeugungsschritt erzeugte neue Authentifizierungssymbolfolge in dem Fall, in dem im Authentifizierungssystem bestimmt wird, dass die beim Authentifizierungsinformation-Übertragungsschritt gesendete neue Authentifizierungssymbolfolge zu dem Typ gehört, wobei

in dem Fall, in dem im Authentifizierungssystem bestimmt wird, dass die vom Authentifizierungsinformation-Übertragungsschritt (S302) gesendete neue Authentifizierungssymbolfolge zu dem Typ gehört, eine Authentifizierung der Endgerätvorrichtung erfolgreich ist, und wobei das Steuerungsverfahren weiter den Schritt umfasst des:

Aktualisierens der Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel gespeichert ist, jedes Mal, wenn die Authentifizierung der Endgerätvorrichtung erfolgreich ist.

14. Steuerungsverfahren für eine Authentifizierungsvorrichtung, die zur Kommunikation mit einer Endgerätvorrichtung für einen Benutzer verbunden ist, um Inhalt oder eine Anwendung zu verwenden, wobei das Steuerungsverfahren umfasst:

einen Schritt (S303) des Erhaltens von mindestens einem Teil von Inhalt, der im Authentifizierungssymbolfolge-Speichermittel zum Speichern einer Authentifizierungssymbolfolge so gespeichert ist, dass er mit Endgerät-Identifikationsinformation zum Identifizieren der Endgerätvorrichtung korreliert ist;

einen Authentifizierungsinformation-Empfangsschritt (S302) des Empfangens, von der Endgerätvorrichtung, der Endgerät-Identifikationsinformation und einer neuen Authentifizierungssymbolfolge, die auf Basis mindestens eines Teils einer Authentifizierungssymbolfolge, die in der Endgerätvorrichtung gespeichert ist, gemäß einer Erzeugungsregel zum Erzeugen einer neuen Authentifizierungssymbolfolge auf Basis einer Authentifizierungssymbolfolge erzeugt wurde;

einen Bestimmungsschritt (S304) des Bestimmens, ob die beim Authentifizierungsinformation-Empfangsschritt empfangene neue Authentifizierungssymbolfolge zu einem Typ einer Authentifizierungssymbolfolge gehört oder nicht, die imstande ist, gemäß der Erzeugungsregel auf Basis mindestens eines Teils der im Authentifizierungssymbolfolge-Speichermittel gespeicherten Authentifizierungssymbolfolge so erzeugt zu werden, dass sie mit der beim Authentifizierungsinformation-Empfangsschritt empfangenen Endgerät-Identifikationsinformation korreliert ist;

einen Hinweisinformation-Übertragungsschritt (S305) des Sendens von Hinweisinformation zum Ermöglichen einer Verwendung des Inhalts oder der Anwendung in der Endgerätvorrichtung an die Endgerätvorrichtung in einem Fall, in dem beim Bestimmungsschritt bestimmt wird, dass die beim Authentifizierungsinformation-Empfangsschritt empfangene neue Authentifizierungssymbolfolge zu dem Typ gehört; und

einen Authentifizierungssymbolfolge-Aktualisierungsschritt (S310) des Aktualisierens der Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel so gespeichert ist, dass sie mit der beim Authentifizierungsinformation-Empfangsschritt empfangenen Endgerät-Identifikationsinformation korreliert ist, auf die beim Authentifizierungsinformation-Empfangsschritt empfangene neue Authentifizierungssymbolfolge in dem Fall, in dem beim Bestimmungsschritt bestimmt wird, dass die beim Authentifizierungsinformation-Empfangsschritt empfangene neue Authentifizierungssymbolfolge zu dem Typ gehört, wobei

in dem Fall, in dem der Bestimmungsschritt (S304) bestimmt, dass die vom Authentifizierungsinformation-Empfangsschritt (S302) empfangene neue Authentifizierungssymbolfolge zu dem Typ gehört, eine Authentifizierung der Endgerätvorrichtung erfolgreich ist, und wobei das Steuerungsverfahren weiter den Schritt umfasst des:

Aktualisierens der Authentifizierungssymbolfolge, die im Authentifizierungssymbolfolge-Speichermittel gespeichert ist, jedes Mal, wenn die Authentifizierung der Endgerätvorrichtung erfolgreich ist.

15. Steuerungsverfahren für ein System zum Bereitstel-

len von Inhalt oder einer Anwendung, das eine Endgerätvorrichtung für einen Benutzer, um den Inhalt oder die Anwendung zu verwenden, und ein Authentifizierungssystem einschließt, umfassend:

ein Steuerungsverfahren für die Endgerätvorrichtung, das nach Anspruch 13 ist; und
ein Steuerungsverfahren für das Authentifizierungssystem, das nach Anspruch 14 ist.

16. Programm zum Bewirken, dass ein Computer als eine Endgerätvorrichtung für einen Benutzer fungiert, um Inhalt oder eine Anwendung zu verwenden, die zur Kommunikation mit einem Authentifizierungssystem verbunden ist, wobei das Programm bewirkt, dass der Computer als die Endgerätvorrichtung nach Anspruch 1 fungiert.

17. Programm zum Bewirken, dass ein Computer als eine Authentifizierungsvorrichtung fungiert, die zur Kommunikation mit einer Endgerätvorrichtung für einen Benutzer verbunden ist, um Inhalt oder eine Anwendung zu verwenden, wobei das Programm bewirkt, dass der Computer als die Authentifizierungsvorrichtung nach Anspruch 2 fungiert.

18. Computerlesbares Informationsspeichermedium, das das Programm nach Anspruch 16 oder 17 speichert.

Revendications

1. Dispositif terminal (10) permettant à un utilisateur d'utiliser un contenu ou une application, pouvant être connecté à des fins de communication à un système d'authentification (22), comprenant :

un moyen de stockage de chaîne de symboles d'authentification (100) pour stocker une chaîne de symboles d'authentification ;
un moyen de génération de chaîne de symboles d'authentification (102) pour générer une nouvelle chaîne de symboles d'authentification sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification (100), conformément à une règle de génération permettant de générer une nouvelle chaîne de symboles d'authentification sur la base d'une chaîne de symboles d'authentification ;
un moyen de transmission d'informations d'authentification (108) pour envoyer des informations d'identification de terminal pour identifier le dispositif terminal et la nouvelle chaîne de symboles d'authentification générée par le moyen de génération de chaîne de symboles d'authentification (102) au système d'authentification (22) ;
un moyen (110) pour recevoir des informations de notification envoyées depuis le système d'authentification (22) dans un cas où il est déterminé dans le système d'authentification (22) que la nouvelle chaîne de symboles d'authentification envoyée depuis le moyen de transmission d'informations d'authentification (108) appartient à un type d'une chaîne de symboles d'authentification qui peut être générée, conformément à la règle de génération, sur la base d'au moins une partie d'une chaîne de symboles d'authentification stockée dans le système d'authentification (22) de façon à être corrélée aux informations d'identification de terminal envoyées par le moyen de transmission d'informations d'authentification (108) ;
un moyen d'autorisation (112) pour autoriser l'utilisation du contenu ou de l'application, sur la base des informations de notification ; et
un moyen de mise à jour de chaîne de symboles d'authentification (114) pour mettre à jour la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification (100) avec la nouvelle chaîne de symboles d'authentification générée par le moyen de génération de chaîne de symboles d'authentification (102) dans le cas où il est déterminé dans le système d'authentification (22) que la nouvelle chaîne de symboles d'authentification envoyée depuis le moyen de transmission d'informations d'authentification (108) appartient au type, dans lequel
dans le cas où il est déterminé dans le système d'authentification (22) que la nouvelle chaîne de symboles d'authentification envoyée depuis le moyen de transmission d'informations d'authentification (108) appartient au type, une authentification du dispositif terminal (10) réussit, et
la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification (100) est mise à jour à chaque fois que l'authentification du dispositif terminal réussit.

2. Dispositif d'authentification (22) pouvant être connecté à des fins de communication à un dispositif terminal (10) pour permettre à un utilisateur d'utiliser un contenu ou une application, comprenant :

un moyen pour obtenir au moins une partie d'un contenu stocké dans un moyen de stockage de chaîne de symboles d'authentification (200) destiné à stocker une chaîne de symboles d'authentification de façon à ce qu'elle soit corrélée à des informations d'identification de ter-

minal pour identifier le dispositif terminal (10) ;
un moyen de réception d'informations d'authentification (202) pour recevoir, du dispositif terminal (10), les informations d'identification de terminal et une nouvelle chaîne de symboles d'authentification générée sur la base d'au moins une partie d'une chaîne de symboles d'authentification stockée dans le dispositif terminal (10), conformément à une règle de génération permettant de générer une nouvelle chaîne de symboles d'authentification sur la base d'une chaîne de symboles d'authentification ;
un moyen de détermination (204) pour déterminer si la nouvelle chaîne de symboles d'authentification reçue par le moyen de réception d'informations d'authentification (202) appartient ou non à un type d'une chaîne de symboles d'authentification qui peut être générée, conformément à la règle de génération, sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification (200) de façon à être corrélée aux informations d'identification de terminal reçues par le moyen de réception d'informations d'authentification (202) ;
un moyen de transmission d'informations de notification (206) pour envoyer des informations de notification pour autoriser l'utilisation du contenu ou de l'application dans le dispositif terminal (10) au dispositif terminal (10) dans un cas où le moyen de détermination (204) détermine que la nouvelle chaîne de symboles d'authentification reçue par le moyen de réception d'informations d'authentification appartient au type ; et
un moyen de mise à jour de chaîne de symboles d'authentification (208) pour mettre à jour la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification (200) de façon à être corrélée aux informations d'identification de terminal reçues par le moyen de réception d'informations d'authentification (202) avec la nouvelle chaîne de symboles d'authentification reçue par le moyen de réception d'informations d'authentification (202), dans le cas où le moyen de détermination (204) détermine que la nouvelle chaîne de symboles d'authentification reçue par le moyen de réception d'informations d'authentification appartient au type, dans lequel
dans le cas où le moyen de détermination (204) détermine que la nouvelle chaîne de symboles d'authentification reçue par le moyen de réception d'informations d'authentification (202) appartient au type, une authentification du dispositif terminal (10) réussit, et
la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification (200) est mise à jour à chaque fois que l'authentification du dispositif terminal réussit.

3. Système (1) de fourniture d'un contenu ou d'une application, comprenant un dispositif terminal (10) permettant à un utilisateur d'utiliser le contenu ou l'application et un système d'authentification (22), dans lequel
le dispositif terminal (10) est conforme à la revendication 1 ;
le système d'authentification (22) est conforme à la revendication 2.

4. Système (1) de fourniture du contenu ou de l'application selon la revendication 3,
dans lequel
le dispositif terminal (10) comprend en outre un premier moyen de stockage d'informations de règle de génération pour stocker des informations de règle de génération pour corréler des informations sur une chaîne de symboles d'authentification et une règle de génération permettant de générer une nouvelle chaîne de symboles d'authentification sur la base d'une chaîne de symboles d'authentification,
le moyen de génération de chaîne de symboles d'authentification (102) est conçu pour spécifier une règle de génération corrélée à la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100), sur la base des informations de règle de génération stockées dans le premier moyen de stockage d'informations de règle de génération, et générer la nouvelle chaîne de symboles d'authentification sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100), conformément à la règle de génération,
le système d'authentification (22) comprend en outre un second moyen de stockage d'informations de règle de génération pour stocker les informations de règle de génération stockées dans le premier moyen de stockage d'informations de règle de génération, et
le moyen de détermination (204) est conçu pour spécifier une règle de génération corrélée à la chaîne de symboles d'authentification stockée dans le second moyen de stockage de chaîne de symboles d'authentification (200), sur la base des informations de règle de génération stockées dans le second moyen de stockage d'informations de règle de génération, et déterminer si la nouvelle chaîne de symboles d'authentification reçue par le moyen de réception d'informations d'authentification (202) appartient ou non à un type d'une chaîne de symboles d'authentification qui peut être générée, conformément à la règle de génération, sur la base d'au moins

une partie de la chaîne de symboles d'authentification stockée dans le second moyen de stockage de chaîne de symboles d'authentification (200) de façon à être corrélée aux informations d'identification de terminal reçues par le moyen de réception d'informations d'authentification (202).

5. Système (1) de fourniture du contenu ou de l'application selon la revendication 4,
dans lequel
les informations de règle de génération sont des informations permettant de corréler une longueur d'une chaîne de symboles d'authentification et une règle de génération permettant de générer une nouvelle chaîne de symboles d'authentification sur la base d'une chaîne de symboles d'authentification,
le moyen de génération de chaîne de symboles d'authentification (102) est conçu pour générer la nouvelle chaîne de symboles d'authentification sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100), conformément à une règle de génération corrélée à une longueur de la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100) et
le moyen de détermination (204) est conçu pour déterminer si la nouvelle chaîne de symboles d'authentification reçue par le moyen de réception d'informations d'authentification appartient ou non à un type d'une chaîne de symboles d'authentification qui peut être générée, conformément à une règle de génération corrélée à une longueur de la chaîne de symboles d'authentification stockée dans le second moyen de stockage de chaîne de symboles d'authentification (200), sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le second moyen de stockage de chaîne de symboles d'authentification (200) de façon à être corrélée aux informations d'identification de terminal reçues par le moyen de réception d'informations d'authentification (202).

6. Système (1) de fourniture du contenu ou de l'application selon la revendication 4,
dans lequel
les informations de règle de génération sont des informations permettant de corréler un type d'un symbole à un emplacement prédéterminé dans une chaîne de symboles d'authentification et une règle de génération permettant de générer une nouvelle chaîne de symboles d'authentification sur la base d'une chaîne de symboles d'authentification,
le moyen de génération de chaîne de symboles d'authentification (102) est conçu pour générer la nouvelle chaîne de symboles d'authentification sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100), conformément à une règle de génération corrélée à un type d'un symbole à l'emplacement prédéterminé dans la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100), et
le moyen de détermination (204) est conçu pour déterminer si la nouvelle chaîne de symboles d'authentification reçue par le moyen de réception d'informations d'authentification (202) appartient ou non à un type d'une chaîne de symboles d'authentification qui peut être générée, conformément à une règle de génération corrélée à un type d'un symbole à l'emplacement prédéterminé dans la chaîne de symboles d'authentification stockée dans le second moyen de stockage de chaîne de symboles d'authentification (200), sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le second moyen de stockage de chaîne de symboles d'authentification (200) de façon à être corrélée aux informations d'identification de terminal reçues par le moyen de réception d'informations d'authentification (202).

7. Système (1) de fourniture du contenu ou de l'application selon l'une quelconque des revendications 3 à 6 dans lequel
le dispositif terminal (10) comprend en outre
un moyen pour guider l'utilisateur pour entrer des informations d'identification d'utilisateur permettant d'identifier l'utilisateur et un mot de passe d'utilisateur, et
un moyen pour envoyer les informations d'identification d'utilisateur et le mot de passe d'utilisateur entrés par l'utilisateur au système d'authentification (22),
le système d'authentification (22) comprend en outre
un moyen de stockage d'informations d'authentification d'utilisateur pour stocker une combinaison des informations d'identification d'utilisateur et du mot de passe d'utilisateur, et
un moyen pour déterminer si la combinaison des informations d'identification d'utilisateur et du mot de passe d'utilisateur envoyée depuis le dispositif terminal est l'une quelconque de combinaisons d'informations d'identification d'utilisateur et d'un mot de passe d'utilisateur stockées dans le moyen de stockage d'informations d'authentification d'utilisateur, et
le système d'authentification (22) est conçu pour fixer la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100) et la chaîne de symboles d'authentification stockée dans le second moyen de stockage de chaîne de symboles d'authentification (200) de façon à être corrélées à

des informations d'identification de terminal corrélées aux informations d'identification d'utilisateur envoyées depuis le dispositif terminal (10), à une même chaîne de symboles d'authentification, dans un cas où il est déterminé que la combinaison des informations d'identification d'utilisateur et du mot de passe d'utilisateur envoyée depuis le dispositif terminal est l'une quelconque des combinaisons des informations d'identification d'utilisateur et du mot de passe d'utilisateur stockées dans le moyen de stockage d'informations d'authentification d'utilisateur.

8. Système (1) de fourniture du contenu ou de l'application selon la revendication 3,
dans lequel
le dispositif terminal (10) comprend en outre
un premier moyen de stockage d'informations de fréquence de mise à jour (118) pour stocker des informations de fréquence de mise à jour concernant un nombre de fois où la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100) est mise à jour, et
un premier moyen de stockage d'informations de règle de génération (116) pour stocker des informations de règle de génération permettant de corréler un nombre de fois où une chaîne de symboles d'authentification est mise à jour et une règle de génération permettant de générer une nouvelle chaîne de symboles d'authentification sur la base d'une chaîne de symboles d'authentification,
le moyen de génération de chaîne de symboles d'authentification (102) est conçu pour spécifier une règle de génération corrélée aux informations de fréquence de mise à jour stockées dans le premier moyen de stockage d'informations de fréquence de mise à jour, sur la base des informations de règle de génération stockées dans le premier moyen de stockage d'informations de règle de génération, et générer la nouvelle chaîne de symboles d'authentification sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100), conformément à la règle de génération,
le système d'authentification (22) comprend en outre
un second moyen de stockage d'informations de fréquence de mise à jour (212) pour stocker des informations de fréquence de mise à jour de façon à ce qu'elles soient corrélées aux informations d'identification de terminal, les informations de fréquence de mise à jour concernant un nombre de fois où la chaîne de symboles d'authentification stockée dans le second moyen de stockage de chaîne de symboles d'authentification de façon à être corrélée aux informations d'identification de terminal est mise à jour, et
un second moyen de stockage d'informations de règle de génération (210) pour stocker les informations de règle de génération stockées dans le premier moyen de stockage d'informations de règle de génération, et
le moyen de détermination (204) est conçu pour spécifier une règle de génération corrélée aux informations de fréquence de mise à jour stockées dans le second moyen de stockage d'informations de fréquence de mise à jour (212) de façon à être corrélées aux informations d'identification de terminal reçues par le moyen de réception d'informations d'authentification (202), sur la base des informations de règle de génération stockées dans le second moyen de stockage d'informations de règle de génération (210), et déterminer si la nouvelle chaîne de symboles d'authentification reçue par le moyen de réception d'informations d'authentification (202) appartient ou non à un type d'une chaîne de symboles d'authentification qui peut être générée, conformément à la règle de génération, sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le second moyen de stockage de chaîne de symboles d'authentification (200) de façon à être corrélée aux informations d'identification de terminal reçues par le moyen de réception d'informations d'authentification (202).

9. Système (1) de fourniture du contenu ou de l'application selon la revendication 8, dans lequel
le dispositif terminal (10) comporte
un moyen pour guider l'utilisateur pour entrer des informations d'identification d'utilisateur permettant d'identifier l'utilisateur et un mot de passe d'utilisateur, et
un moyen pour envoyer les informations d'identification d'utilisateur et le mot de passe d'utilisateur entrés par l'utilisateur au système d'authentification,
le système d'authentification comprend en outre
un moyen de stockage d'informations d'authentification d'utilisateur pour stocker une combinaison des informations d'identification d'utilisateur et du mot de passe d'utilisateur, et
un moyen pour déterminer si la combinaison des informations d'identification d'utilisateur et du mot de passe d'utilisateur envoyée depuis le dispositif terminal est ou non l'une quelconque de combinaisons d'informations d'identification d'utilisateur et d'un mot de passe d'utilisateur stockées dans le moyen de stockage d'informations d'authentification d'utilisateur, et
le système d'authentification (22) est conçu pour fixer la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100) et la chaîne de symboles d'authentification stockée dans le second moyen de stockage de chaîne de symboles d'authentification (200) de façon à être corrélées à des informations d'identification de terminal corrélées aux informations d'identification d'utilisateur en-

voyées depuis le dispositif terminal (10), à une même chaîne de symboles d'authentification, et fixer les informations de fréquence de mise à jour stockées dans le premier moyen de stockage d'informations de fréquence de mise à jour (118) et les informations de fréquence de mise à jour stockées dans le second moyen de stockage d'informations de fréquence de mise à jour (212) de façon à être corrélées aux informations d'identification de terminal corrélées aux informations d'identification d'utilisateur envoyées depuis le dispositif terminal (10), à une même fréquence de mise à jour, dans un cas où il est déterminé que la combinaison des informations d'identification d'utilisateur et du mot de passe d'utilisateur envoyée depuis le dispositif terminal (10) est l'une quelconque des combinaisons des informations d'identification d'utilisateur et du mot de passe d'utilisateur stockées dans le moyen de stockage d'informations d'authentification d'utilisateur.

10. Système (1) de fourniture du contenu ou de l'application selon l'une quelconque des revendications 3 à 9, dans lequel
la règle de génération comprend une règle dans laquelle un symbole à un emplacement donné dans une chaîne de symboles d'authentification doit être extrait, et
le moyen de génération de chaîne de symboles d'authentification (102) comprend un moyen d'extraction (104) pour extraire, conformément à la règle de génération, un ou plusieurs symboles de la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification, et générer la nouvelle chaîne de symboles d'authentification sur la base des un ou plusieurs symboles extraits par le moyen d'extraction (104).

11. Système (1) de fourniture du contenu ou de l'application selon l'une quelconque des revendications 3 à 10, dans lequel
la règle de génération comprend au moins l'une parmi une règle pour convertir un seul symbole d'une chaîne de symboles d'authentification en un seul symbole, une règle pour convertir un seul symbole d'une chaîne de symboles d'authentification en une pluralité de symboles, une règle pour convertir une pluralité de symboles d'une chaîne de symboles d'authentification en un seul symbole, et une règle pour convertir une pluralité de symboles d'une chaîne de symboles d'authentification en une pluralité de symboles, et
le moyen de génération de chaîne de symboles d'authentification (102) comprend un moyen de conversion (106) pour convertir au moins une partie de la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100) conformément à la règle de génération pour obtenir un ou plusieurs symboles, et générer la nouvelle chaîne de symboles d'authentification sur la base des un ou plusieurs symboles obtenus par le moyen de conversion (106).

12. Système (1) de fourniture du contenu ou de l'application selon l'une quelconque des revendications 3 à 11, dans lequel
la règle de génération comprend une règle dans laquelle un ou plusieurs symboles basé(s) sur au moins une partie d'une chaîne de symboles d'authentification doit/doivent être inclus(s) à un emplacement donné dans la nouvelle chaîne de symboles d'authentification, et
le moyen de génération de chaîne de symboles d'authentification (102) est conçu pour générer, conformément à la règle de génération, une chaîne de symboles comprenant un ou plusieurs symboles basés sur au moins une partie de la chaîne de symboles d'authentification stockée dans le premier moyen de stockage de chaîne de symboles d'authentification (100) comme étant la nouvelle chaîne de symboles d'authentification.

13. Procédé de commande d'un dispositif terminal permettant à un utilisateur d'utiliser un contenu ou une application, connecté à des fins de communication à un système d'authentification, le procédé de commande comprenant :

une étape consistant à obtenir une chaîne de symboles d'authentification stockée dans un moyen de stockage de chaîne de symboles d'authentification pour stocker la chaîne de symboles d'authentification ;
une étape de génération de chaîne de symboles d'authentification (S301) consistant à générer une nouvelle chaîne de symboles d'authentification sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification, conformément à une règle de génération permettant de générer une nouvelle chaîne de symboles d'authentification sur la base d'une chaîne de symboles d'authentification ;
une étape de transmission d'informations d'authentification (S302) consistant à envoyer des informations d'identification de terminal pour identifier le dispositif terminal et la nouvelle chaîne de symboles d'authentification générée à l'étape de génération de chaîne de symboles d'authentification au système d'authentification ;
une étape de réception d'informations de notification (S305) envoyées depuis le système d'authentification dans un cas où il est déterminé dans le système d'authentification que la nou-

velle chaîne de symboles d'authentification envoyée à l'étape de transmission d'informations d'authentification appartient à un type d'une chaîne de symboles d'authentification qui peut être générée, conformément à la règle de génération, sur la base d'au moins une partie d'une chaîne de symboles d'authentification stockée dans le système d'authentification de façon à être corrélée aux informations d'identification de terminal envoyées à l'étape de transmission d'informations d'authentification ;

une étape d'autorisation (S308) consistant à autoriser l'utilisation du contenu ou de l'application, sur la base des informations de notification ; et

une étape de mise à jour de chaîne de symboles d'authentification (S307) consistant à mettre à jour la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification avec la nouvelle chaîne de symboles d'authentification générée à l'étape de génération de chaîne de symboles d'authentification dans le cas où il est déterminé dans le système d'authentification que la nouvelle chaîne de symboles d'authentification envoyée à l'étape de transmission d'informations d'authentification appartient au type, dans lequel

dans le cas où il est déterminé dans le système d'authentification que la nouvelle chaîne de symboles d'authentification envoyée par l'étape de transmission d'informations d'authentification (S302) appartient au type, une authentification du dispositif terminal réussit, et l'étape de commande comprenant en outre l'étape de :

mise à jour de la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification à chaque fois que l'authentification du dispositif terminal réussit.

14. Procédé de commande d'un dispositif d'authentification connecté à des fins de communication à un dispositif terminal pour permettre à un utilisateur d'utiliser un contenu ou une application, le procédé de commande comprenant :

une étape (S303) d'obtention d'au moins une partie d'un contenu stocké dans un moyen de stockage de chaîne de symboles d'authentification pour stocker une chaîne de symboles d'authentification de façon à ce qu'elle soit corrélée à des informations d'identification de terminal permettant d'identifier le dispositif terminal ;

une étape de réception d'informations d'authentification (S302) consistant à recevoir, du dispositif terminal, les informations d'identification de terminal et une nouvelle chaîne de symboles d'authentification générée sur la base d'au moins une partie d'une chaîne de symboles d'authentification stockée dans le dispositif terminal, conformément à une règle de génération permettant de générer une nouvelle chaîne de symboles d'authentification, sur la base d'une chaîne de symboles d'authentification ;

une étape de détermination (S304) consistant à déterminer si la nouvelle chaîne de symboles d'authentification reçue à l'étape de réception d'informations d'authentification appartient ou non à un type d'une chaîne de symboles d'authentification qui peut être générée, conformément à la règle de génération, sur la base d'au moins une partie de la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification de façon à être corrélée aux informations d'identification de terminal reçues à l'étape de réception d'informations d'authentification ;

une étape de transmission d'informations de notification (S305) consistant à envoyer des informations de notification pour autoriser l'utilisation du contenu ou de l'application dans le dispositif terminal au dispositif terminal dans un cas où il est déterminé à l'étape de détermination que la nouvelle chaîne de symboles d'authentification reçue à l'étape de réception d'informations d'authentification appartient au type ; et

une étape de mise à jour de chaîne de symboles d'authentification (S310) consistant à mettre à jour la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification de façon à être corrélée aux informations d'identification de terminal reçues à l'étape de réception d'informations d'authentification avec la nouvelle chaîne de symboles d'authentification reçue à l'étape de réception d'informations d'authentification, dans le cas où il est déterminé à l'étape de détermination que la nouvelle chaîne de symboles d'authentification reçue à l'étape de réception d'informations d'authentification appartient au type, dans lequel

dans le cas où l'étape de détermination (S304) détermine que la nouvelle chaîne de symboles d'authentification reçue par l'étape de réception d'informations d'authentification (S302) appartient au type, une authentification du dispositif terminal réussit, et le procédé de commande comprend en outre l'étape de :

mise à jour de la chaîne de symboles d'authentification stockée dans le moyen de stockage de chaîne de symboles d'authentification à chaque fois que l'authentification du dispositif terminal réussit.

15. Procédé de commande d'un système de fourniture d'un contenu ou d'une application comprenant un dispositif terminal permettant à un utilisateur d'utiliser le contenu ou l'application et un système d'authentification, comprenant :

un procédé de commande du dispositif terminal selon la revendication 13 ; et
un procédé de commande du système d'authentification selon la revendication 14.

16. Programme destiné à faire fonctionner un ordinateur comme un dispositif terminal permettant à un utilisateur d'utiliser un contenu ou une application, connecté à des fins de communication à un système d'authentification, le programme étant destiné à faire fonctionner l'ordinateur comme le dispositif terminal selon la revendication 1.

17. Programme destiné à faire fonctionner un ordinateur comme un dispositif d'authentification connecté à des fins de communication à un dispositif terminal permettant à un utilisateur d'utiliser un contenu ou une application, le programme étant destiné à faire fonctionner l'ordinateur comme le dispositif d'authentification selon la revendication 2.

18. Support de stockage d'informations lisible par ordinateur stockant le programme selon la revendication 16 ou 17.

FIG.1

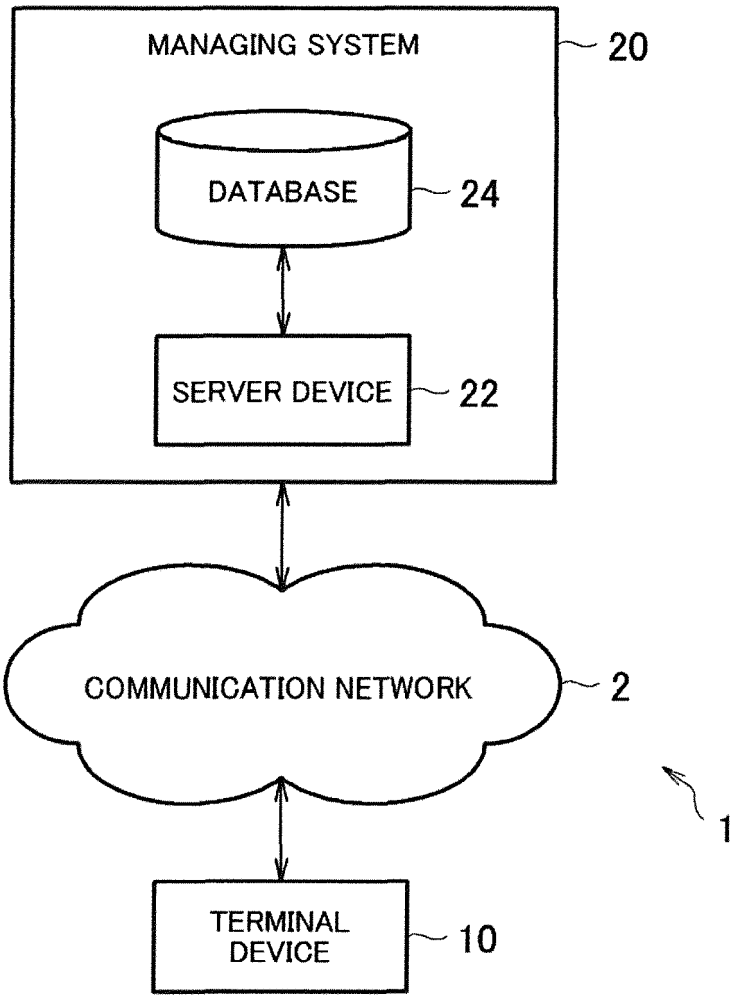
MANAGING SYSTEM
20
DATABASE
24
SERVER DEVICE
22
COMMUNICATION NETWORK
2
1
TERMINAL DEVICE
10

FIG.2

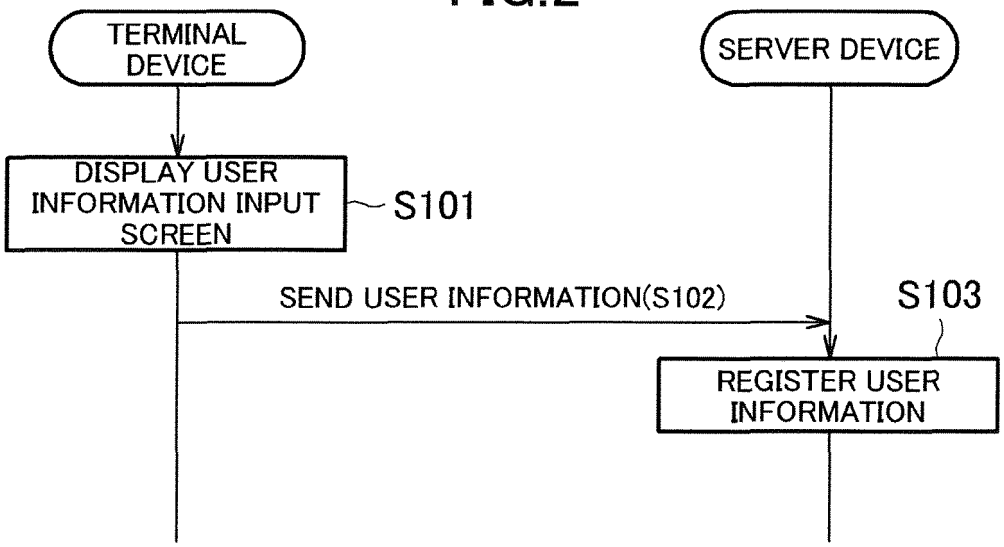
TERMINAL DEVICE
SERVER DEVICE
DISPLAY USER INFORMATION INPUT SCREEN
S101
SEND USER INFORMATION(S102)
S103
REGISTER USER INFORMATION

FIG.3

USER ID	USER PASSWORD	NAME	ADDRESS	CREDIT CARD INFORMATION
U00001	P00001	― ― ―	― ― ―	― ― ―
U00002	P00002	― ― ―	― ― ―	― ― ―
...	...	...	...	...

FIG.4

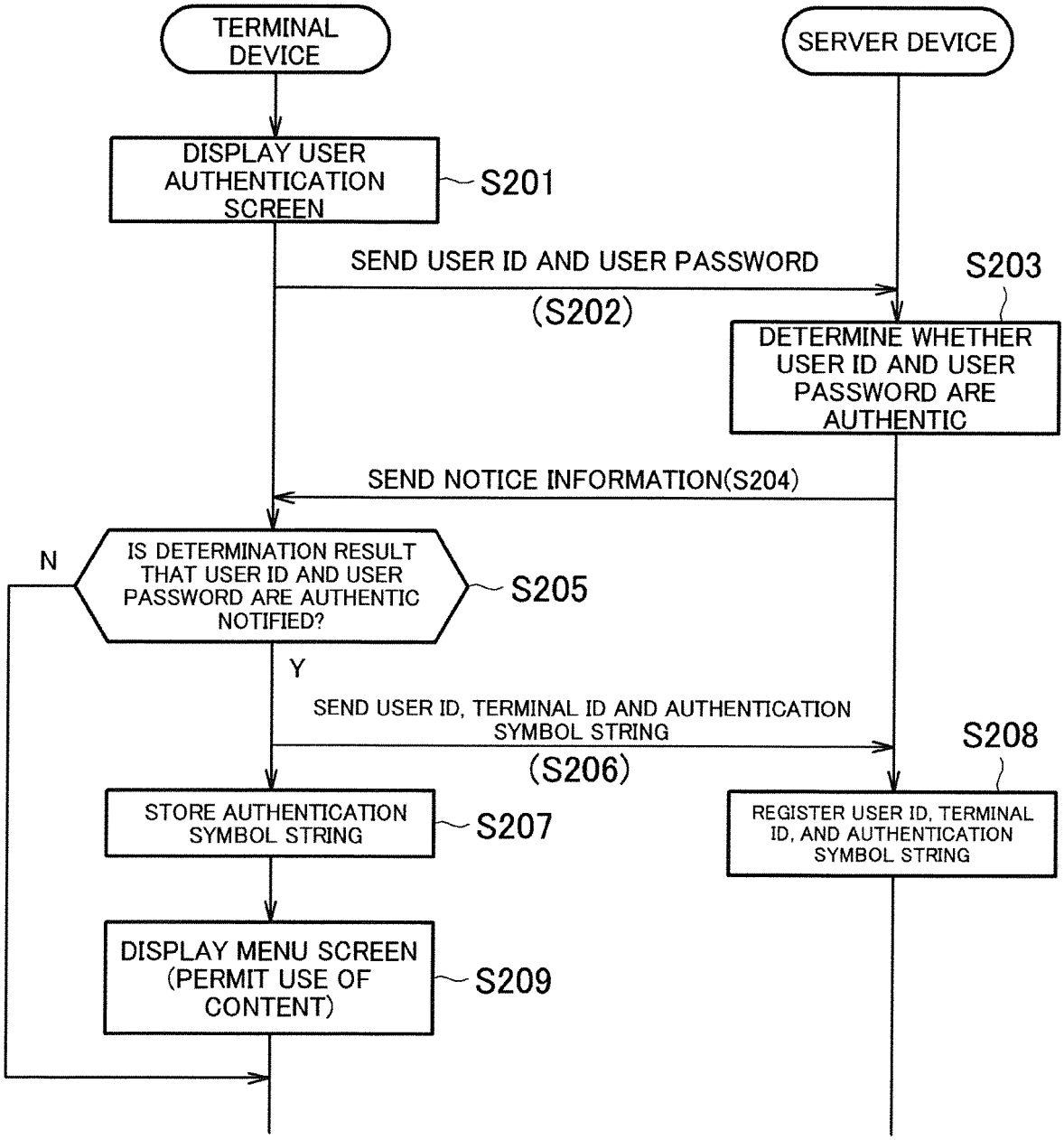

FIG.5

TERMINAL ID	T00001
AUTHENTICATION SYMBOL STRING	ABCDE

FIG.6

USER ID	TERMINAL ID	AUTHENTICATION SYMBOL STRING	CONTENT/APPLICATION INFORMATION
U00001	T00001	ABCDE	———
U00002	T00002	PQRSTUV	———
...	...	...	...

FIG.7

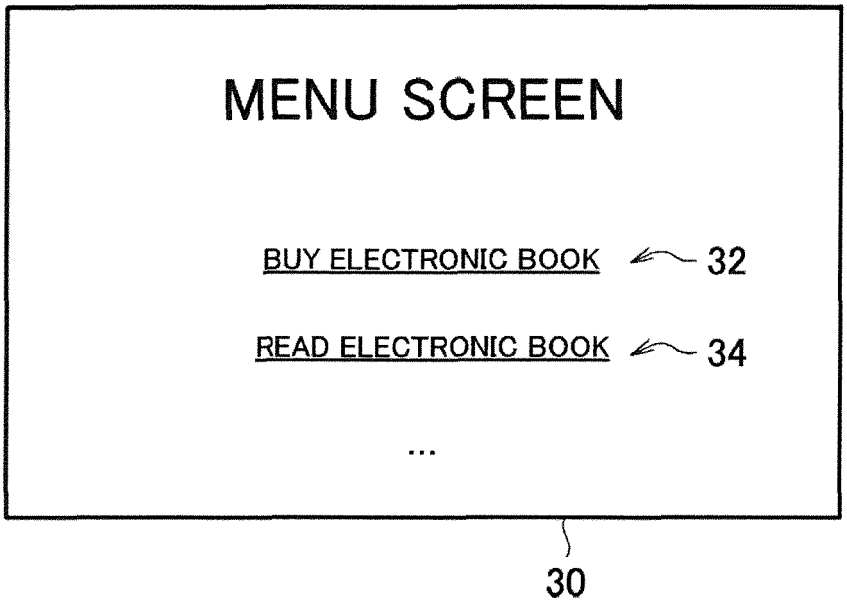

FIG.8

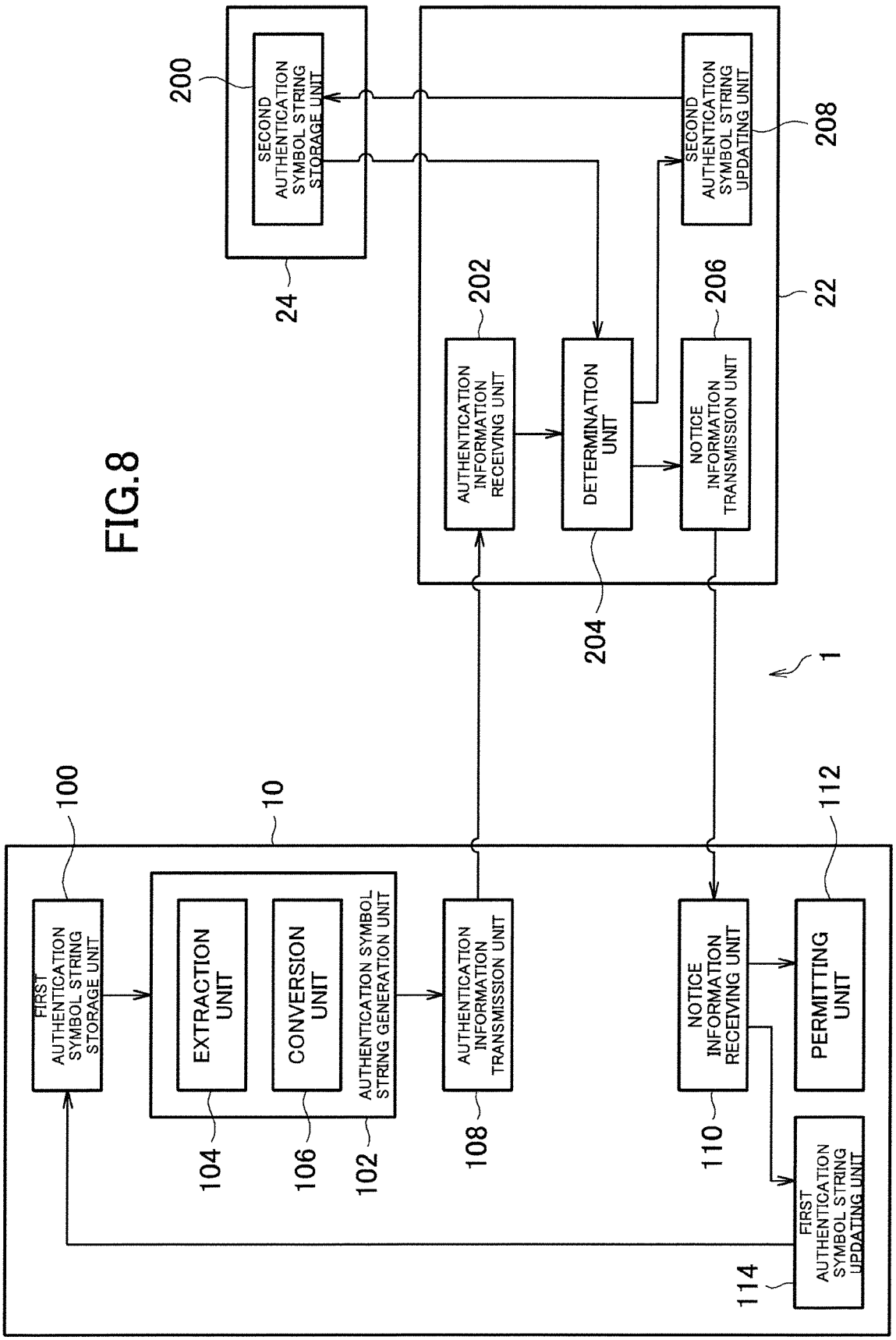
200
SECOND AUTHENTICATION SYMBOL STRING STORAGE UNIT
24
SECOND AUTHENTICATION SYMBOL STRING UPDATING UNIT
208
22
202
AUTHENTICATION INFORMATION RECEIVING UNIT
DETERMINATION UNIT
206
NOTICE INFORMATION TRANSMISSION UNIT
204
1
100
10
112
FIRST AUTHENTICATION SYMBOL STRING STORAGE UNIT
EXTRACTION UNIT
CONVERSION UNIT
AUTHENTICATION SYMBOL STRING GENERATION UNIT
AUTHENTICATION INFORMATION TRANSMISSION UNIT
NOTICE INFORMATION RECEIVING UNIT
PERMITTING UNIT
104
106
102
108
110
FIRST AUTHENTICATION SYMBOL STRING UPDATING UNIT
114

FIG.9

	AUTHENTICATION SYMBOL STRING	NEW AUTHENTICATION SYMBOL STRING
EXAMPLE (1)	ABCDE	EXPT4H368B
EXAMPLE (2)	ABCDE	DEXPT4H368B
EXAMPLE (3)	ABCDE	CEXPT4H368B
EXAMPLE (4)	ABCDE (CONVERSION)	FXPT4H368B
EXAMPLE (5)	ABCDE (CONVERSION)	FGXPT4H368B
EXAMPLE (6)	ABCDE (CONVERSION)	KXPT4H368B
EXAMPLE (7)	ABCDE (CONVERSION)	MLSXPT4H368B

FIG.10

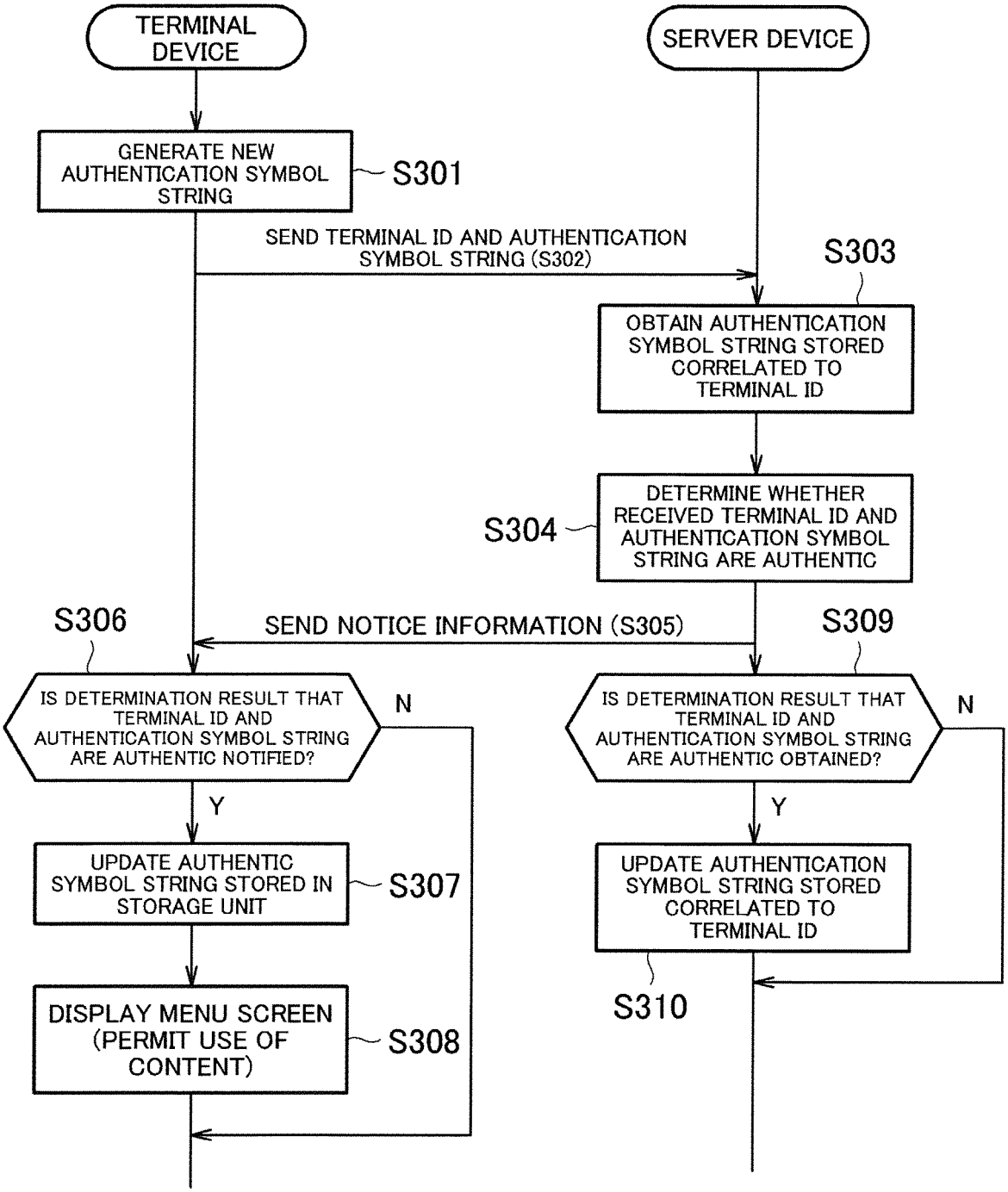
TERMINAL DEVICE
SERVER DEVICE
GENERATE NEW AUTHENTICATION SYMBOL STRING
S301
SEND TERMINAL ID AND AUTHENTICATION SYMBOL STRING (S302)
S303
OBTAIN AUTHENTICATION SYMBOL STRING STORED CORRELATED TO TERMINAL ID
S304
DETERMINE WHETHER RECEIVED TERMINAL ID AND AUTHENTICATION SYMBOL STRING ARE AUTHENTIC
S306
SEND NOTICE INFORMATION (S305)
S309
IS DETERMINATION RESULT THAT TERMINAL ID AND AUTHENTICATION SYMBOL STRING ARE AUTHENTIC NOTIFIED?
N
Y
IS DETERMINATION RESULT THAT TERMINAL ID AND AUTHENTICATION SYMBOL STRING ARE AUTHENTIC OBTAINED?
N
Y
UPDATE AUTHENTIC SYMBOL STRING STORED IN STORAGE UNIT
S307
UPDATE AUTHENTICATION SYMBOL STRING STORED CORRELATED TO TERMINAL ID
S310
DISPLAY MENU SCREEN (PERMIT USE OF CONTENT)
S308

FIG.11

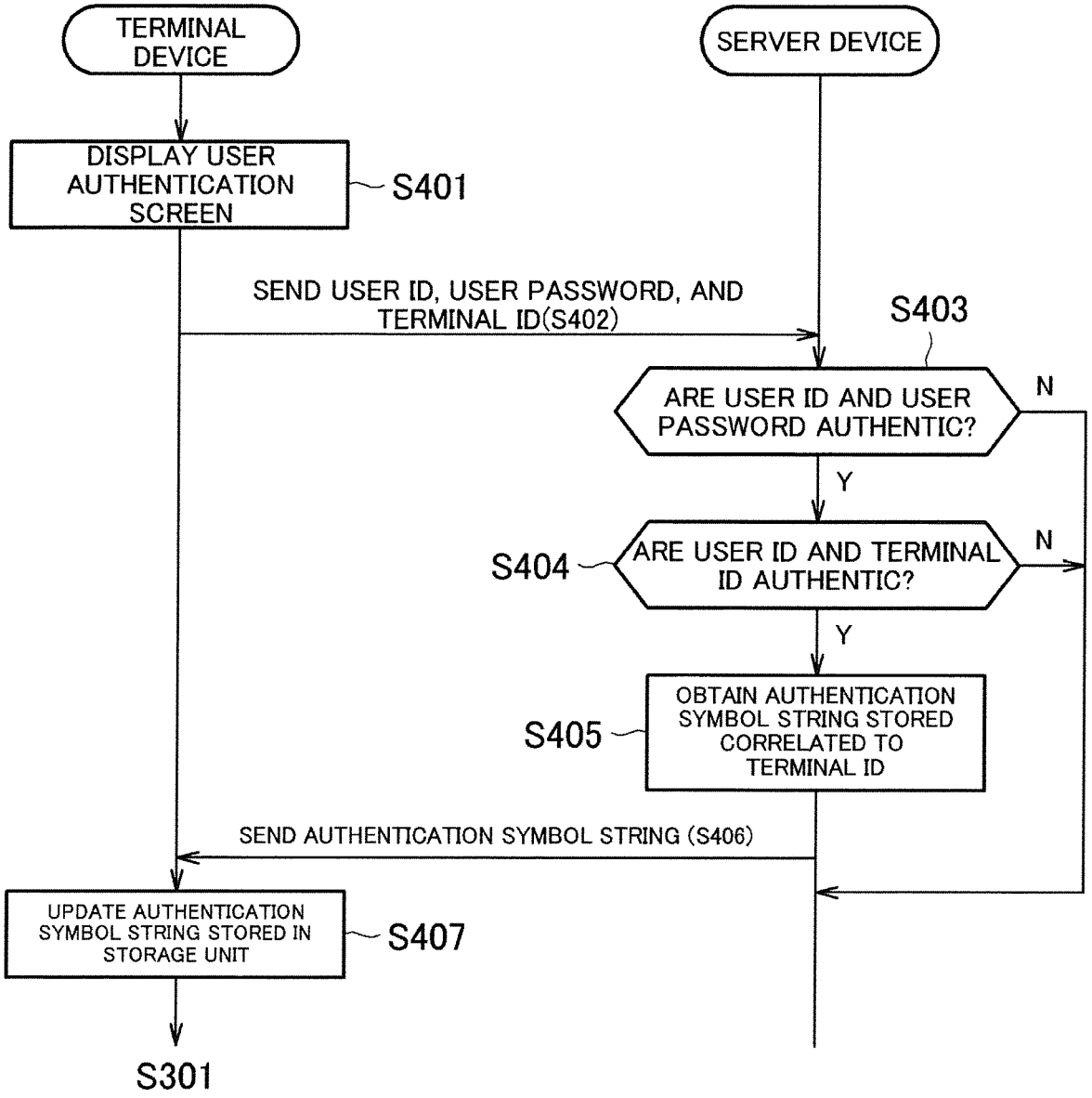
TERMINAL DEVICE
SERVER DEVICE
DISPLAY USER AUTHENTICATION SCREEN
S401
SEND USER ID, USER PASSWORD, AND TERMINAL ID(S402)
S403
ARE USER ID AND USER PASSWORD AUTHENTIC?
N
Y
S404
ARE USER ID AND TERMINAL ID AUTHENTIC?
N
Y
S405
OBTAIN AUTHENTICATION SYMBOL STRING STORED CORRELATED TO TERMINAL ID
SEND AUTHENTICATION SYMBOL STRING (S406)
UPDATE AUTHENTICATION SYMBOL STRING STORED IN STORAGE UNIT
S407
S301

FIG.12

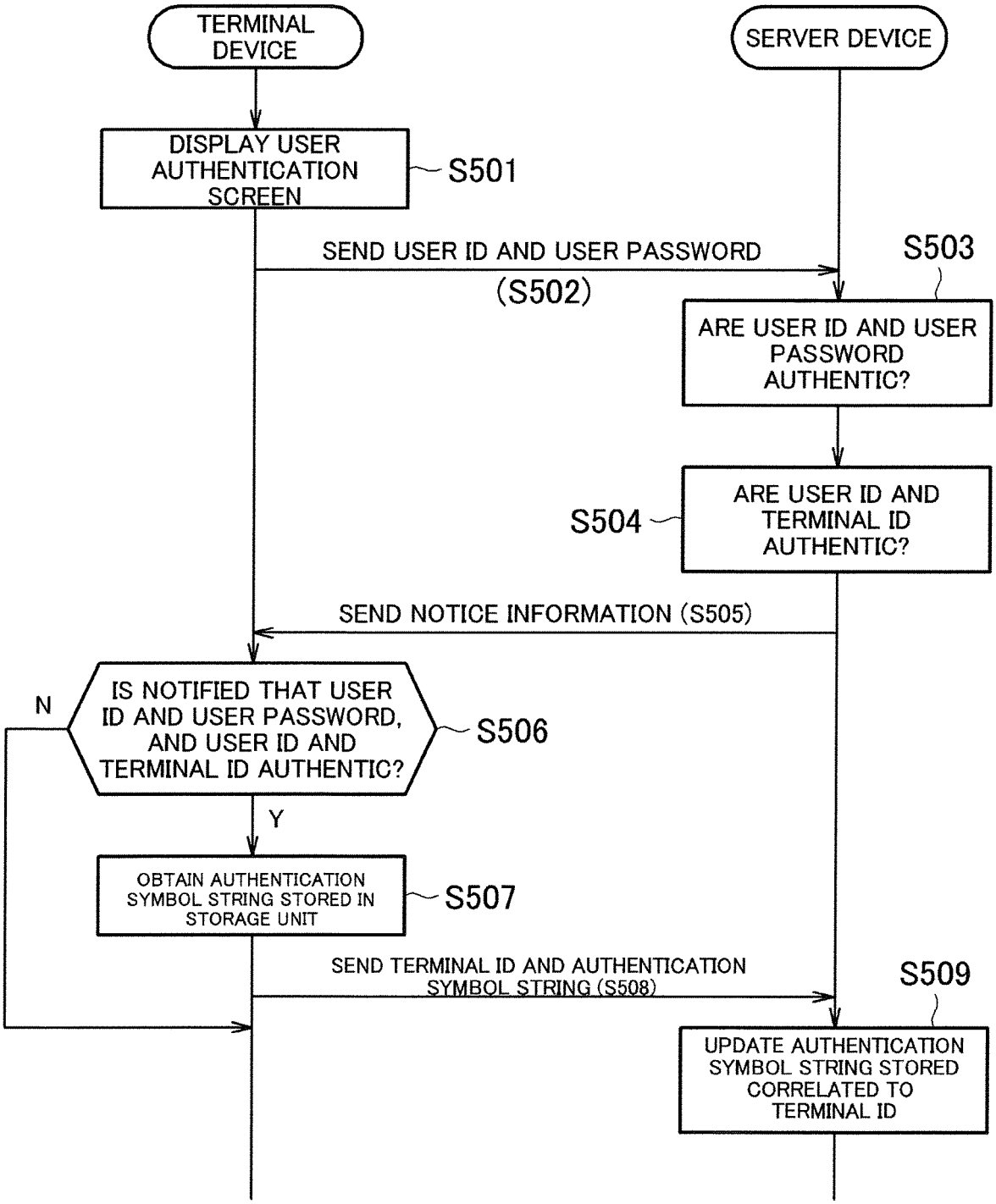
TERMINAL DEVICE
SERVER DEVICE
DISPLAY USER AUTHENTICATION SCREEN
S501
SEND USER ID AND USER PASSWORD (S502)
S503
ARE USER ID AND USER PASSWORD AUTHENTIC?
S504
ARE USER ID AND TERMINAL ID AUTHENTIC?
SEND NOTICE INFORMATION (S505)
N
IS NOTIFIED THAT USER ID AND USER PASSWORD, AND USER ID AND TERMINAL ID AUTHENTIC?
S506
Y
OBTAIN AUTHENTICATION SYMBOL STRING STORED IN STORAGE UNIT
S507
SEND TERMINAL ID AND AUTHENTICATION SYMBOL STRING (S508)
S509
UPDATE AUTHENTICATION SYMBOL STRING STORED CORRELATED TO TERMINAL ID

FIG.13

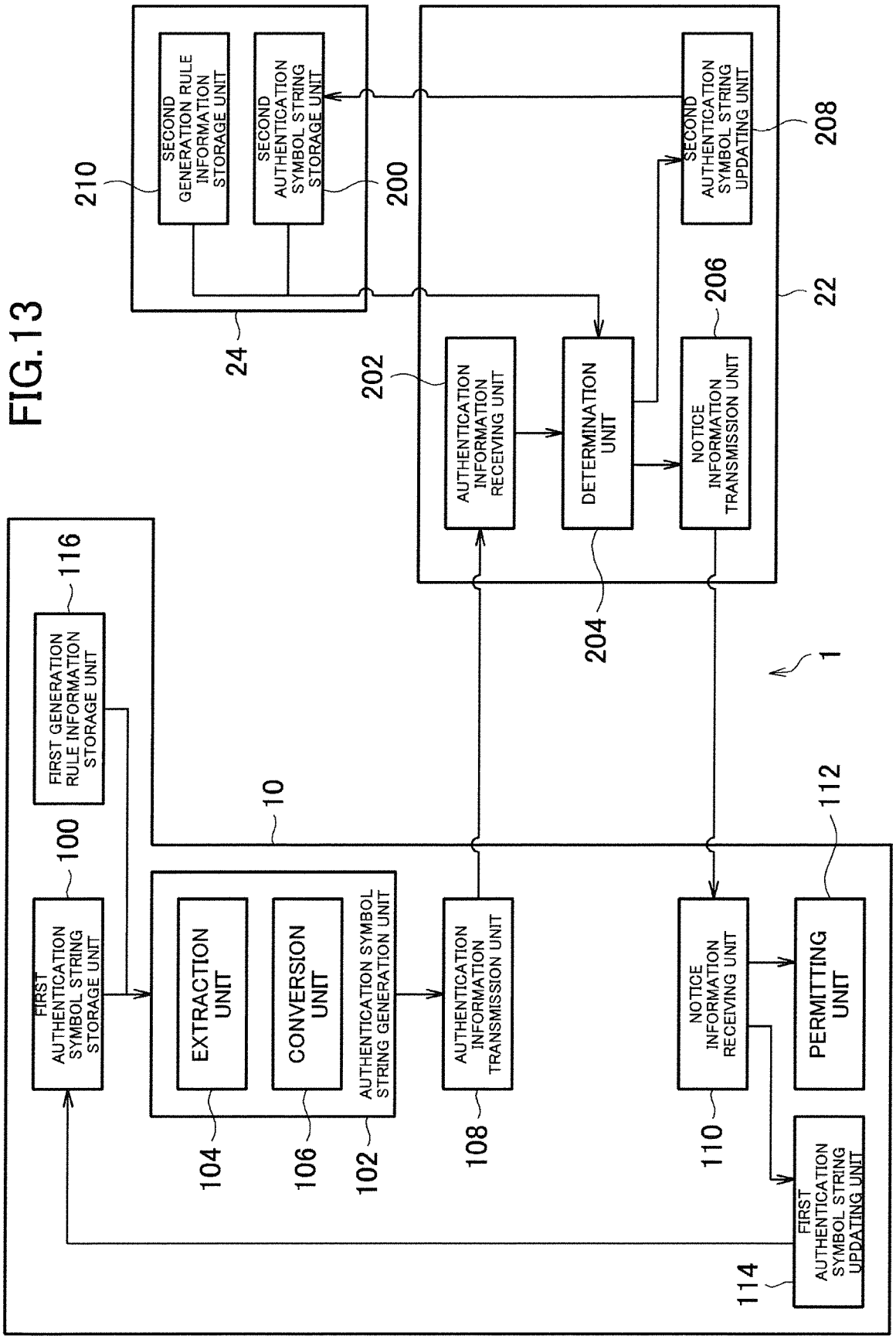
SECOND GENERATION RULE INFORMATION STORAGE UNIT
SECOND AUTHENTICATION SYMBOL STRING STORAGE UNIT
SECOND AUTHENTICATION SYMBOL STRING UPDATING UNIT
210
200
208
24
22
206
202
AUTHENTICATION INFORMATION RECEIVING UNIT
DETERMINATION UNIT
NOTICE INFORMATION TRANSMISSION UNIT
204
1
116
FIRST GENERATION RULE INFORMATION STORAGE UNIT
10
112
100
FIRST AUTHENTICATION SYMBOL STRING STORAGE UNIT
EXTRACTION UNIT
CONVERSION UNIT
AUTHENTICATION SYMBOL STRING GENERATION UNIT
AUTHENTICATION INFORMATION TRANSMISSION UNIT
NOTICE INFORMATION RECEIVING UNIT
PERMITTING UNIT
104
106
102
108
110
FIRST AUTHENTICATION SYMBOL STRING UPDATING UNIT
114

FIG.14

AUTHENTICATION SYMBOL STRING LENGTH(x)	GENERATION RULE
$x < Xa$	GENERATION RULE A
$Xa \leqq x$	GENERATION RULE B

FIG.15

SYMBOL TYPE	GENERATION RULE
SYMBOL GROUP A	GENERATION RULE A
SYMBOL GROUP B	GENERATION RULE B

FIG.16

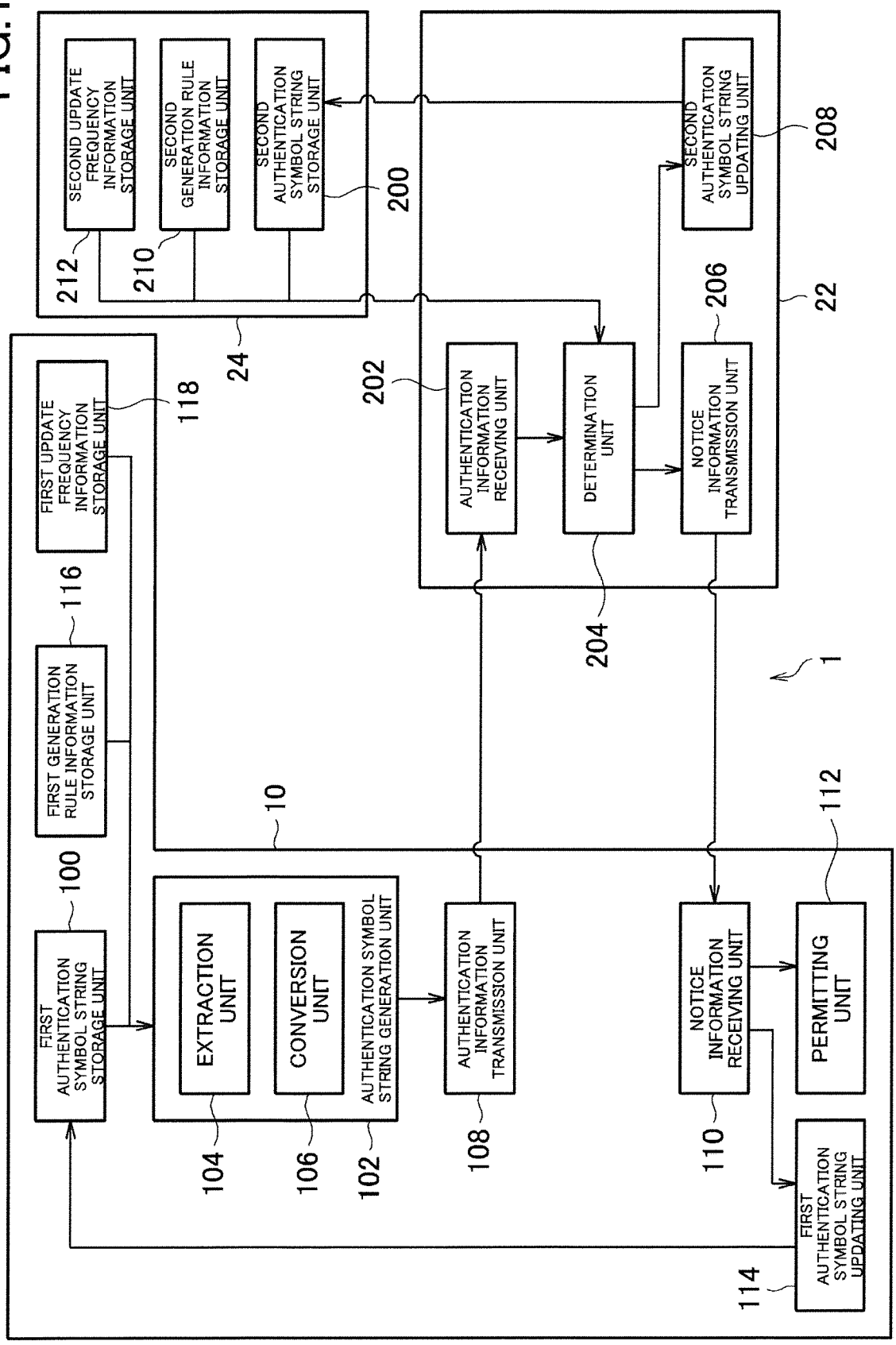
SECOND UPDATE FREQUENCY INFORMATION STORAGE UNIT
SECOND GENERATION RULE INFORMATION STORAGE UNIT
SECOND AUTHENTICATION SYMBOL STRING STORAGE UNIT
SECOND AUTHENTICATION SYMBOL STRING UPDATING UNIT
208
212
210
200
22
206
24
202
AUTHENTICATION INFORMATION RECEIVING UNIT
DETERMINATION UNIT
NOTICE INFORMATION TRANSMISSION UNIT
FIRST UPDATE FREQUENCY INFORMATION STORAGE UNIT
118
116
204
1
FIRST GENERATION RULE INFORMATION STORAGE UNIT
10
112
100
EXTRACTION UNIT
CONVERSION UNIT
AUTHENTICATION SYMBOL STRING GENERATION UNIT
AUTHENTICATION INFORMATION TRANSMISSION UNIT
NOTICE INFORMATION RECEIVING UNIT
PERMITTING UNIT
FIRST AUTHENTICATION SYMBOL STRING STORAGE UNIT
104
106
102
108
110
FIRST AUTHENTICATION SYMBOL STRING UPDATING UNIT
114

FIG.17

UPDATE FREQUENCY INFORMATION	2

FIG.18

UPDATE FREQUENCY(y)	GENERATION RULE
$y < Ya$	GENERATION RULE A
$Ya \leqq y$	GENERATION RULE B

FIG.19

USER ID	TERMINAL ID	AUTHENTICATION SYMBOL STRING	UPDATE FREQUENCY INFORMATION	CONTENT/APPLICATION INFORMATION
U00001	T00001	ABCDE	2	———
U00002	T00002	PQRSTUV	5	———
...	...	...	...	...

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 1677205 A1 **[0004]**